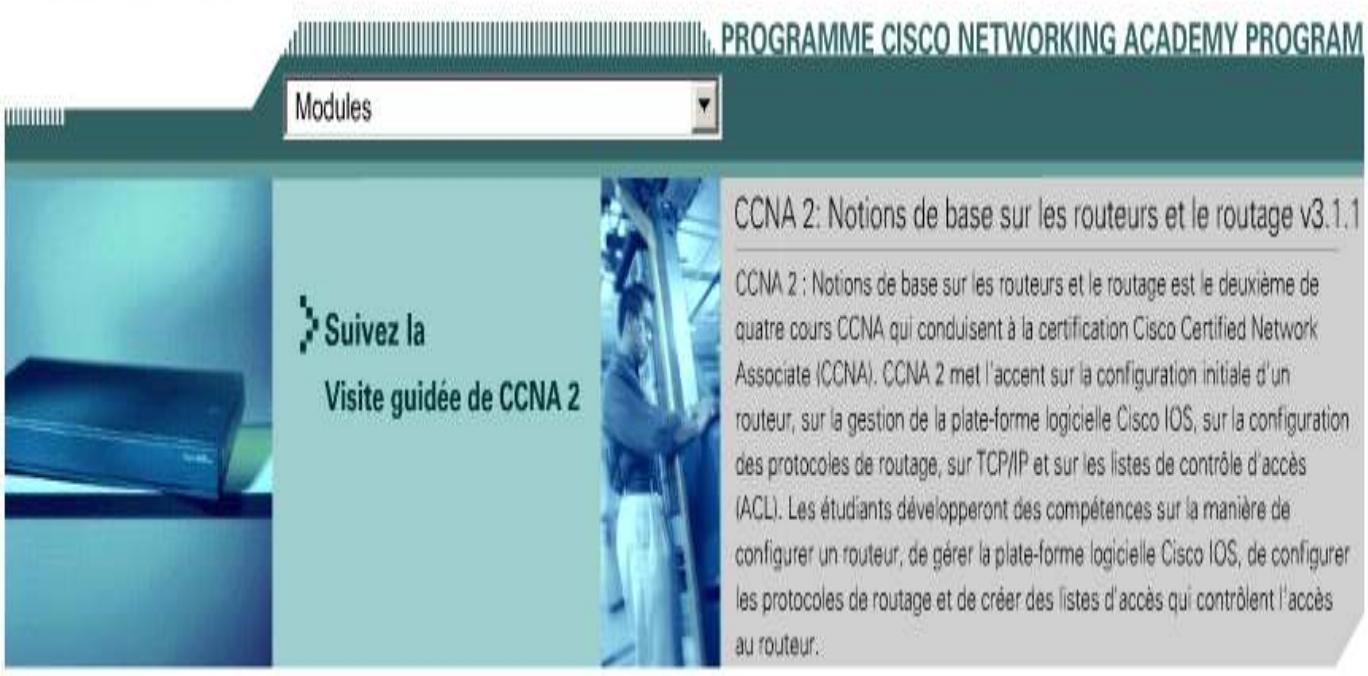


Vue d'ensemble

Un réseau WAN est un réseau de communication de données qui couvre une zone géographique étendue. Ces réseaux possèdent des caractéristiques importantes qui les distinguent des réseaux locaux, ou LAN. Le premier cours de ce module présente une vue d'ensemble des technologies et des protocoles propres aux réseaux WAN. Il explique également ce qui différencie les réseaux WAN et les réseaux LAN, et ce qui les rapproche.

Il est important de comprendre les différents composants de la couche physique des routeurs. C'est en effet cette compréhension qui étaiera les autres connaissances et compétences nécessaires pour configurer des routeurs et gérer des réseaux routés. Ce module traite en détail des composants physiques internes et externes des routeurs. Il décrit également les techniques qui permettent de connecter physiquement les diverses interfaces de routeur.

À la fin de ce module, les étudiants doivent être en mesure de:

- Identifier les organisations qui régissent les normes relatives aux réseaux WAN
- Expliquer la différence entre un WAN et un LAN, ainsi que le type d'adresses qu'utilise chacun de ces réseaux
- Décrire le rôle d'un routeur au sein d'un réseau WAN
- Identifier les composants internes d'un routeur et décrire leurs fonctions
- Décrire les caractéristiques physiques d'une routeur
- Identifier les principaux ports d'un routeur
- Connecter correctement les ports Ethernet, WAN série et console

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
1.1	Réseaux WAN
1.2	Routeurs

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception d'un LAN simple à l'aide de la technologie Cisco • Conception d'un interréseau simple à l'aide de la technologie Cisco • Sélection de services WAN répondant aux besoins des clients	• Configuration de protocoles de routage d'après les besoins des utilisateurs • Mise en œuvre de protocoles WAN simples		• Comparaison des principales caractéristiques des environnements LAN • Description des composants d'équipements réseau • Évaluation des principales caractéristiques des réseaux WAN

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception d'un interréseau simple à l'aide de la technologie Cisco • Sélection de protocoles WAN répondant aux besoins de la conception	• Configuration de protocoles de routage d'après les besoins des • Mise en œuvre de protocoles WAN simples		• Évaluation des caractéristiques des environnements LAN

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
	• Établissement de communication entre un équipement terminal et la plate-forme logicielle IOS du routeur, et utilisation de l'IOS en vue de l'analyse du système • Description et installation du matériel et du logiciel requis pour pouvoir communiquer via un réseau	• Définition et description de la structure des réseaux informatiques et des technologies associées • Description du matériel et du logiciel requis pour pouvoir communiquer via un réseau • Identification des principales caractéristiques des technologies et des configurations WAN (Wide Area Networking) courantes, et différences par rapport aux technologies LAN les plus • Description du rôle d'un routeur au sein d'un réseau WAN • Identification des principaux composants internes et externes d'un routeur, et description des fonctionnalités associées

1.1 Réseaux WAN

1.1.1 Introduction aux réseaux WAN

Un réseau WAN est un réseau de communication de données qui couvre une zone géographique étendue, comme un département, une région ou un pays par exemple. Les réseaux WAN utilisent la plupart du temps les moyens de transmission fournis par les opérateurs télécom. [1]

Les principales caractéristiques des réseaux WAN sont les suivantes:

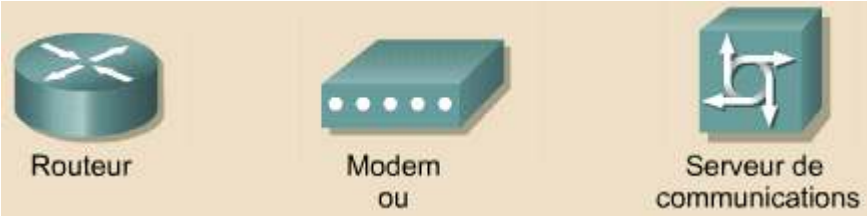
- Ils relient des équipements géographiquement éloignés.
- Pour établir un lien ou une connexion entre plusieurs sites, ils utilisent les services de porteuse d'opérateurs tels que RBOC (Regional Bell Operating Company), Sprint, MCI et VPM Internet Services, Inc.
- Ils utilisent divers types de connexions série pour accéder à la bande passante sur de vastes zones géographiques.

Distance entre les unités	Emplacement des hôtes	Nom
10m	Pièce	Réseau LAN Salle de classe
100m	Bâtiment	Réseau LAN École
1000m = 1km	Campus	Réseau LAN Université
10,000m = 10km	Ville	Réseau métropolitain
100,000m = 100km	Pays	Réseau WAN Cisco Systems, Inc.
1,000,000m = 1,000km	Continent	Réseau WAN Afrique
10,000,000m = 10,000km	Planète	Réseau WAN Internet
100,000,000m = 100,000km	Systèmes terre-lune	Réseau WAN Satellites terrestres et artificiels

Un réseau WAN se distingue d'un réseau LAN de diverses façons. Par exemple, contrairement à un réseau LAN, qui relie des stations de travail, des périphériques, des terminaux et d'autres unités situés dans un même bâtiment ou dans un lieu rapproché, un réseau WAN assure des connexions de données sur une zone géographique étendue. Les entreprises utilisent les réseaux WAN pour interconnecter leurs divers sites de façon à pouvoir échanger des informations entre des bureaux distants.

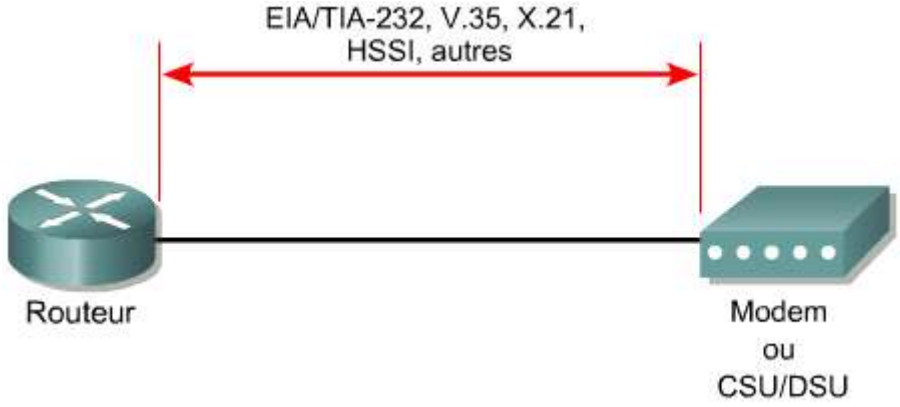
Un réseau WAN fonctionne au niveau de la couche physique et de la couche liaison de données du modèle de référence OSI. Il interconnecte des réseaux LAN qui sont généralement séparés par de vastes étendues géographiques. Les réseaux WAN permettent l'échange de paquets et de trames de données entre les routeurs et les commutateurs qui constituent le réseau jusqu'aux réseaux LAN qu'ils prennent en charge.

Les équipements suivants sont utilisés dans les réseaux WAN: [2] [3]



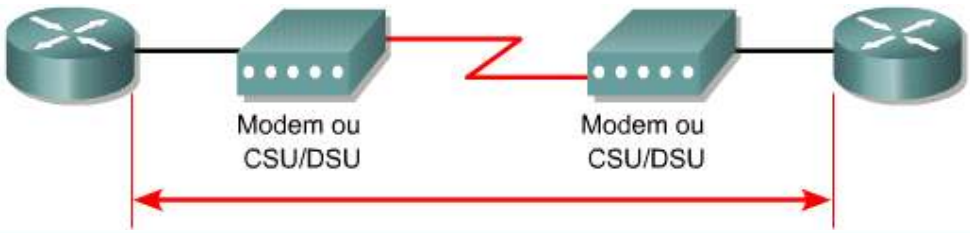
Les réseaux WAN :
- couvrent une vaste région géographique,
- permet de choisir une connexion série de faible coût et de faible prix ou une connexion ATM ou Fibre Optique plus rapide, mais plus chère,
- assurent une connectivité continue ou intermittente.

- Des routeurs, qui offrent de nombreux services, y compris l'interconnexion, ainsi que des ports d'interface de réseau WAN.
- Le terme «modems» inclut des services d'interface de qualité voix, des unités CSU/DSU servant d'interface pour les services T1-E1 ; des adaptateurs de terminal/terminaison de réseau 1 (NT1) servant d'interface pour les services RNIS (Réseau Numérique à Intégration de Services).
- Des serveurs de communication, qui concentrent les communications utilisateur entrantes et sortantes via le RTC.



ETTD Équipement terminal de traitement de données Unité utilisateur avec interface de connexion à la liaison WAN	ETCD Équipement de terminaison de circuit de données Extrémité de l'unité de communication côté fournisseur du réseau WAN

Les protocoles de liaison de données WAN spécifient la façon dont les trames sont transportées entre les systèmes sur une même liaison. Il s'agit notamment des protocoles conçus pour fonctionner avec des services point à point, multipoints et commutés multi-accès, tels que les services Frame Relay. Les normes de réseau WAN sont définies et gérées par plusieurs autorités reconnues, dont les organismes suivants:



- HDLC (High Level Data Link Control)
- Frame Relay - Successeur de X.25
- PPP (protocole point-à-point)
- RNIS (Réseau Numérique à Intégration de Services) (signal de liaison de données)

- L'UIT-T (*Union Internationale des Télécommunications – secteur de normalisation des Télécommunications*), anciennement appelée CCITT (*Comité Consultatif International Télégraphique et Téléphonique*).
- L'Organisation internationale de normalisation (ISO).
- L'Internet Engineering Task Force (IETF).
- L'Electrical Industries Association (EIA).

Activité de média interactive

Glisser-Positionner : Identification des unités réseau

À la fin de cette activité, l'étudiant sera en mesure de comprendre les réseaux WAN.

1.1 Réseaux WAN

1.1.2 Introduction aux routeurs dans un réseau WAN

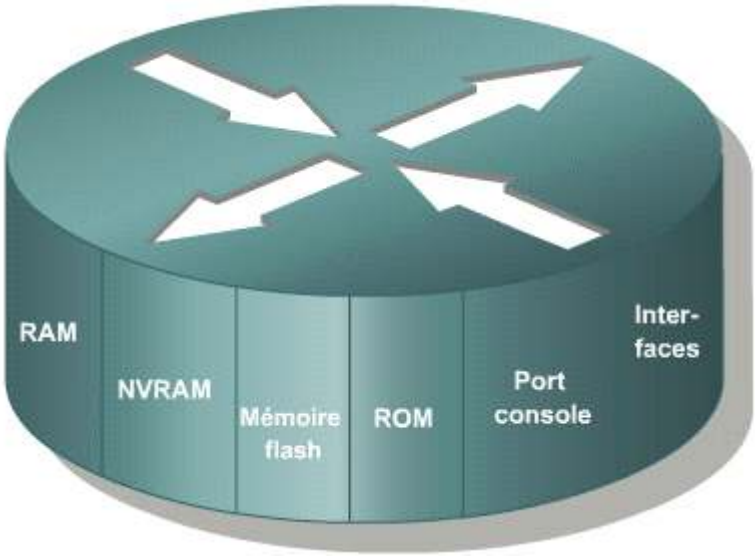
Un routeur est un type spécial d'ordinateur. Il possède les mêmes composants de base qu'un ordinateur de bureau standard. Il est doté d'un processeur (UC), de mémoire, d'un système de bus, ainsi que de diverses interfaces d'entrée/sortie. Cependant, les routeurs sont conçus pour assurer des fonctions très spécifiques que n'effectuent pas en général les ordinateurs de bureau. Par exemple, des routeurs peuvent se connecter, assurer la communication entre deux réseaux et déterminer le meilleur chemin pour les données à travers les réseaux connectés.

À l'instar des ordinateurs qui ont besoin d'un système d'exploitation pour exécuter les applications, les routeurs doivent être équipés d'une plate-forme logicielle IOS (*Internetworking Operating Software*) pour exécuter les fichiers de configuration. Ces fichiers contiennent les instructions et les paramètres qui contrôlent le trafic entrant et sortant des routeurs. Plus précisément, en utilisant des protocoles de routage, les routeurs décident du meilleur chemin pour les paquets. Le fichier de configuration spécifie toutes les informations pour l'installation et l'utilisation correctes des protocoles de routage -et routés- sélectionnés ou activés sur le routeur.

Ce cours démontre comment créer des fichiers de configuration à l'aide des commandes IOS, afin de faire exécuter au routeur un certain nombre de fonctions réseau essentielles. Le fichier de configuration de routeur peut sembler complexe à première vue, mais vous comprendrez mieux son contenu à l'issue de ce cours.

Les principaux composants internes du routeur sont la mémoire vive (RAM), la mémoire vive rémanente (NVRAM), la mémoire morte (ROM) et les interfaces. 1

RAM – La mémoire RAM est utilisée pour les informations de table de routage, la mémoire cache à commutation rapide, la configuration courante et les files d'attente de paquets.
NVRAM – La mémoire NVRAM est utilisée pour stocker un fichier de configuration de démarrage/sauvegarde.
Flash – La mémoire flash est utilisée pour stocker les images de l'IOS.
ROM – La mémoire ROM est utilisée pour stocker de manière permanente le code de diagnostic de démarrage.
Console – Le port console fournit un accès physique pour la configuration initiale.
Interfaces – Les interfaces fournissent la connectivité LAN et WAN.



La mémoire vive, également appelée mémoire vive dynamique (DRAM), possède les caractéristiques et les fonctions suivantes:

- elle contient les tables de routage,
- elle contient le cache ARP,
- elle contient la mémoire cache à commutation rapide,
- elle effectue la mise en mémoire tampon des paquets (RAM partagée),
- elle gère les files d'attente de paquets,
- elle sert de mémoire temporaire pour le fichier de configuration à la mise sous tension du routeur,
- elle perd son contenu à la mise hors tension ou au redémarrage du routeur.

La mémoire vive rémanente (NVRAM) possède les caractéristiques et fonctions suivantes:

- elle assure le stockage du fichier de configuration de démarrage,
- elle conserve son contenu à la mise hors tension ou au redémarrage du routeur.

La mémoire flash possède les caractéristiques et fonctions suivantes:

- elle contient l'image du système d'exploitation (IOS),
- elle permet de mettre à jour le logiciel sans suppression ni remplacement de puces sur le processeur,
- elle conserve son contenu à la mise hors tension ou au redémarrage du routeur,
- elle peut stocker plusieurs versions de la plate-forme logicielle IOS,
- elle constitue un type de ROM programmable et effaçable électroniquement (EEPROM).

La mémoire morte (ROM) possède les caractéristiques et fonctions suivantes:

- elle gère les instructions du test automatique de mise sous tension (POST),
- elle stocke le programme d'amorçage (bootstrap) et le logiciel de système d'exploitation de base,
- elle nécessite un remplacement des puces enfichables sur la carte mère pour procéder aux mises à jour logicielles.

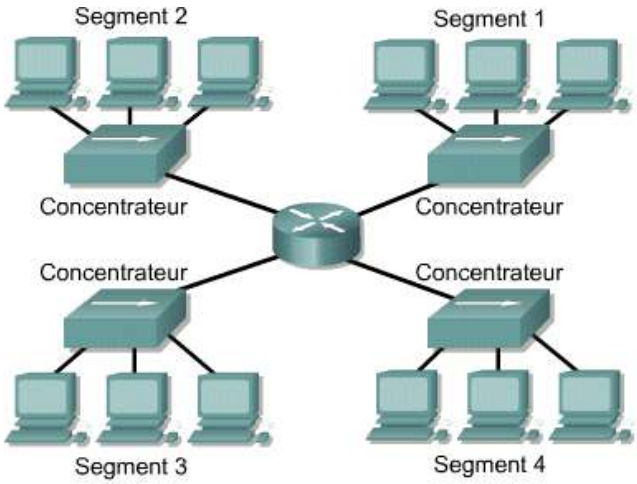
Les interfaces possèdent les caractéristiques et fonctions suivantes:

- elles connectent le routeur au réseau pour l'entrée et la sortie des paquets,
- elles peuvent se trouver sur la carte mère ou sur un module séparé.

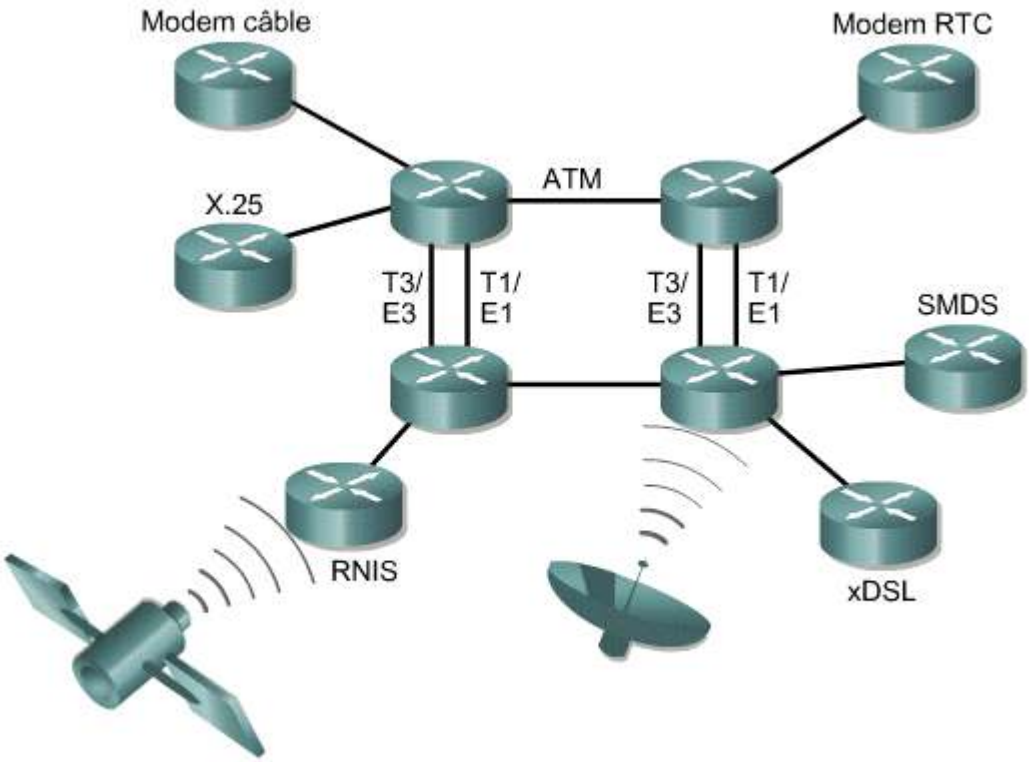
1.1 Réseaux WAN

Routeur de réseaux LAN et WAN

Bien qu'un routeur puisse servir pour segmenter des réseaux LAN, son utilisation première est celle d'une unité WAN. [1] [2]

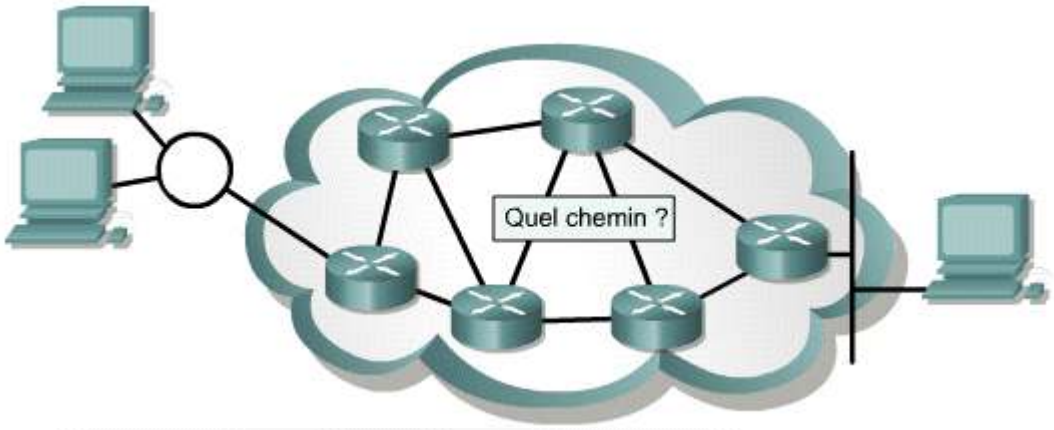


- Gestion plus facile, fonctionnalité accrue, multiples chemins actifs
- Domaines de diffusion plus petits
- Fonctionne au niveau de la couche 3



Les routeurs sont dotés à la fois d'interfaces LAN et WAN. En fait, les technologies WAN sont fréquemment utilisées pour connecter des routeurs, et ceux-ci communiquent les uns avec les autres via des connexions WAN. [3] Les routeurs constituent le backbone des grands intranets et d'Internet. Ils fonctionnent sur la couche 3 du modèle OSI, et prennent des décisions en fonction des adresses réseau. Les deux fonctions principales d'un routeur sont de sélectionner le meilleur chemin pour les

paquets et de commuter ces paquets vers l'interface appropriée. Pour ce faire, les routeurs créent des tables de routage et échangent des informations sur le réseau avec d'autres routeurs.



La couche 3 recherche le meilleur chemin dans l'interréseau.

L'administrateur peut gérer des tables de routage en configurant des routes statiques, mais ces dernières sont habituellement gérées de manière dynamique par un protocole de routage qui échange des informations sur la topologie réseau avec d'autres routeurs.

Si, par exemple, l'ordinateur (x) a besoin de communiquer avec l'ordinateur (y) d'un côté du monde, et avec l'ordinateur (z) dans un autre emplacement distant, une fonction de routage pour la circulation des informations est nécessaire, ainsi que des chemins redondants pour une fiabilité accrue. De nombreuses technologies et décisions relatives à la conception des réseaux découlent de cette volonté de faire communiquer les ordinateurs x, y et z.

Un interréseau correctement configuré fournit les éléments suivants:

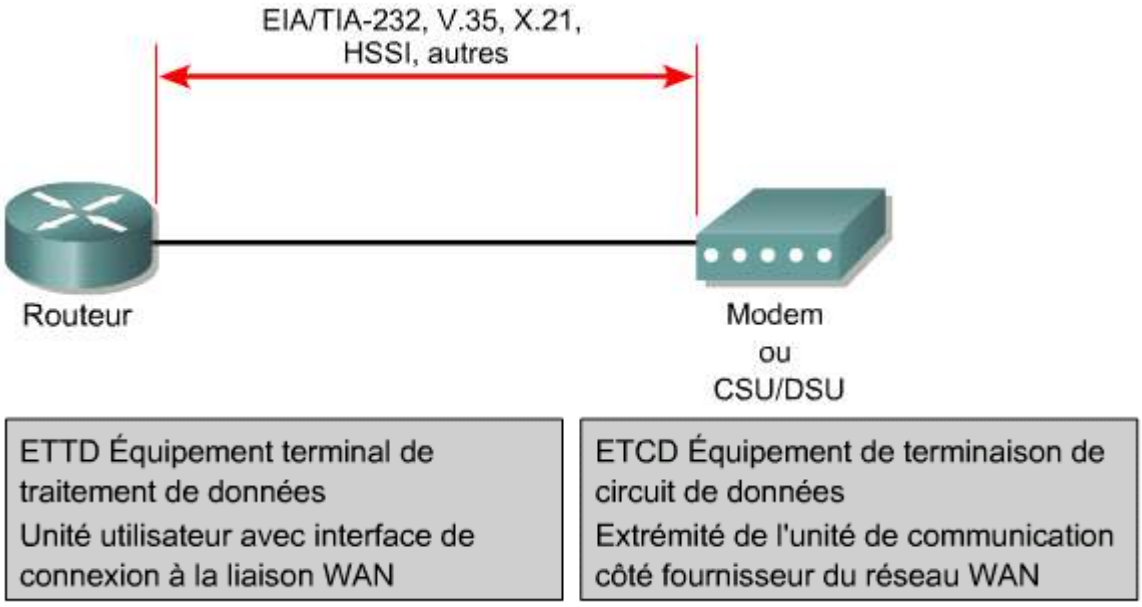
- un adressage cohérent de bout en bout,
- des adresses représentant les topologies réseau,
- une sélection du meilleur chemin,
- un routage dynamique ou statique,
- la commutation.

1.1 Réseaux WAN

1.1.4 Rôle d'un routeur au sein d'un réseau WAN

Nous avons déjà dit qu'un réseau WAN fonctionne sur la couche physique et sur la couche liaison de données. Cela ne veut pas dire que les cinq autres couches du modèle OSI sont absentes d'un réseau WAN, mais simplement que les caractéristiques qui distinguent un réseau WAN d'un réseau LAN se situent en général au niveau de la couche physique et de la couche liaison de données. Autrement dit, les normes et les protocoles des couches 1 et 2 des réseaux WAN sont différents de ceux des mêmes couches des réseaux LAN.

La couche physique WAN décrit l'interface entre l'ETTD (*équipement terminal de traitement de données*) et l'ETCD (*équipement de terminaison de circuit de données*). En règle générale, l'ETCD est le réseau du fournisseur d'accès et l'ETTD, l'unité connectée. Selon ce modèle, les services fournis à l'ETTD le sont par l'intermédiaire d'un modem ou d'une unité CSU/DSU. 1



La fonction principale d'un routeur est le routage. Le routage s'effectue au niveau de la couche réseau - la couche 3, mais si un réseau WAN fonctionne au niveau des couches 1 et 2, le routeur est-il alors une unité LAN ou une unité WAN ?

La réponse est « les deux », comme c'est souvent le cas dans le domaine des réseaux. Un routeur peut être exclusivement une unité LAN, exclusivement une unité WAN, se situer à la limite entre un réseau LAN et un réseau WAN ou être à la fois une unité LAN et une unité WAN.

L'un des rôles d'un routeur au sein d'un réseau WAN consiste à router les paquets au niveau de la couche 3, mais il pourrait en être de même sur un réseau LAN. Par conséquent, le routage n'est pas un rôle exclusif d'un routeur sur un réseau WAN. Lorsqu'un routeur utilise les protocoles et normes de la couche physique et de la couche liaison de données qui sont associés aux réseaux WAN, il fonctionne comme une unité WAN. Le rôle principal d'un routeur dans un WAN n'est donc pas le routage, mais la compatibilité des connexions vers et entre les diverses normes physiques et de liaison de données d'un réseau WAN. Par exemple, un routeur peut être doté d'une interface RNIS qui utilise l'encapsulation PPP et d'une interface série terminant une ligne E1 qui utilise l'encapsulation Frame Relay. Le routeur doit pouvoir transférer un flux de bits d'un type de service, comme RNIS, vers un autre, comme E1, et changer l'encapsulation de liaison de données de PPP en Frame Relay.

Les protocoles WAN des couches 1 et 2 sont traités en détail plus loin dans ce cours, mais vous trouverez ci-dessous la liste des principaux protocoles et normes pour référence.

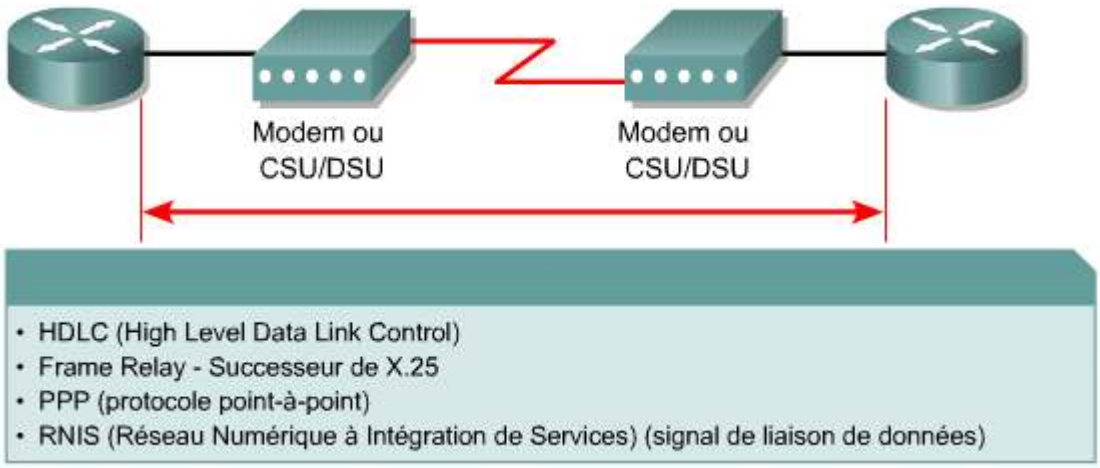
Normes et protocoles de la couche physique WAN:

- EIA/TIA-232
- EIA/TIA-449
- V.24
- V.35

- X.21
- G.703
- EIA-530
- RNIS
- T1, T3, E1 et E3
- xDSL
- SONET (OC-3, OC-12, OC-48, OC-192)

Normes et protocoles de la couche liaison de données WAN: 2

- HDLC (High-level Data Link Control)
- Frame Relay
- PPP (protocole point à point)
- SDLC (Synchronous Data Link Control)
- SLIP (Serial Line Internet Protocol)
- X.25
- ATM
- LAPB
- LAPD
- LAPF

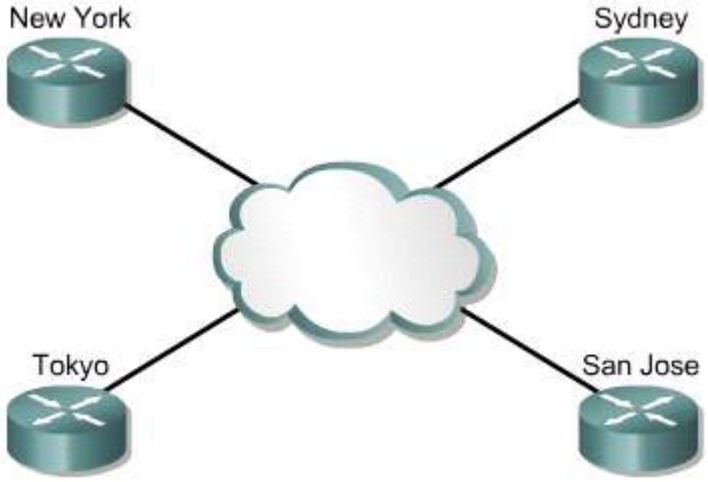


1.1 Réseaux WAN

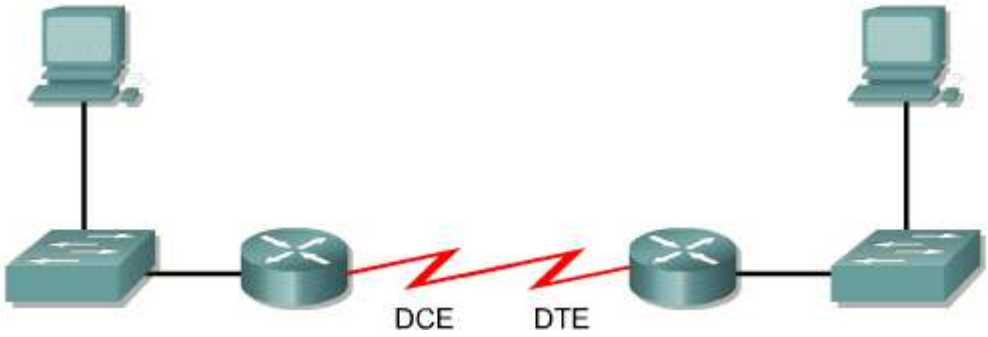
1.1.5 Philosophie de l'Académie en matière de travaux pratiques

Dans le TP, tous les réseaux sont connectés à l'aide de câbles série ou Ethernet et les étudiants peuvent voir et toucher tous les équipements. 1Dans le monde réel, les câbles série ne sont pas connectés dos-à-dos comme pour les besoins de notre TP. En situation réelle, un routeur pourrait se trouver à New York, et un autre à Sydney. Un administrateur situé à Sydney devra

se connecter au routeur de New York via le nuage WAN afin de dépanner le routeur de New York.



Dans cette configuration de TP, les unités qui constituent le nuage WAN sont simulées par les câbles de connexion directe entre les ETTD et ETCD. 2La connexion d'une interface de routeur s0/0 à une autre interface de routeur s0/1 simule l'ensemble du nuage du circuit.



Activité de média interactive

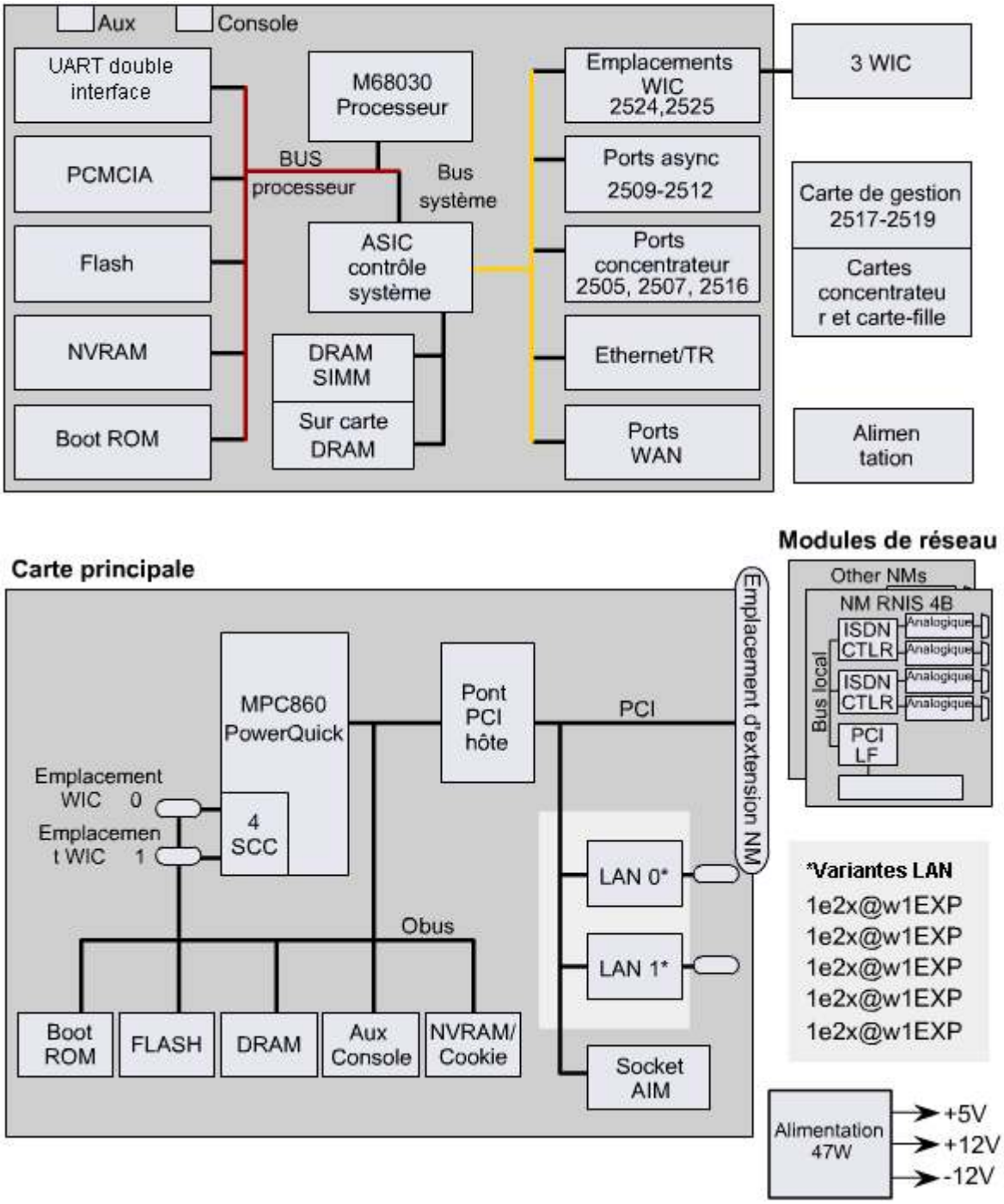
Glisser-Positionner : Installation de l'équipement de TP

À la fin de cette activité, l'étudiant doit savoir connecter tous les câbles et toutes les unités dans l'ordre approprié pour créer la topologie de TP CCNA.

1.2 Routeurs

1.2.1 Composants internes des routeurs

tien que l'architecture exacte d'un routeur varie selon le modèle, la présente section présente les principaux composants internes de ces équipements Les figures 1et 2illustrent les composants internes de certains des modèles de routeur Cisco. Les composants communs sont abordés dans les paragraphes ci-dessous.



UC: Le processeur (UC) exécute les instructions du système d'exploitation IOS. Ses principales fonctions sont, entre autres, l'initialisation du système, le routage et le contrôle de l'interface réseau. L'UC est un microprocesseur. Les grands routeurs sont généralement multiprocesseurs.

RAM: La mémoire vive (RAM) sert à stocker les données de la table de routage, de la mémoire cache à commutation rapide, de la configuration courante et des files d'attente de paquets. Dans la plupart des routeurs, la mémoire vive fournit un espace d'exécution pour l'IOS exécutable et ses sous-systèmes. La mémoire vive est en général divisée au niveau logique en mémoire processeur principale et en mémoire d'entrée/sortie (E/S) partagée. La mémoire d'E/S partagée est répartie entre les interfaces pour le stockage temporaire des paquets. Le contenu de la mémoire vive est perdu lorsque l'alimentation est coupée. La mémoire vive est généralement constituée de mémoire vive dynamique (DRAM) et peut être mise à niveau en ajoutant des modules mémoire DIMM (Dual In-Line Memory Modules).

Mémoire flash: La mémoire flash est utilisée pour le stockage d'une image complète de la plate-forme logicielle Cisco IOS. Le routeur obtient normalement l'IOS par défaut de la mémoire flash. Ces images peuvent être mises à niveau en chargeant en mémoire flash une nouvelle image. L'IOS peut être au format non compressé ou compressé. Dans la plupart des routeurs, une copie exécutable de l'IOS est transférée vers la mémoire vive au cours du processus de démarrage. Dans d'autres

routeurs, l'IOS peut être exécuté directement à partir de la mémoire flash. L'ajout ou le remplacement des modules SIMM de mémoire flash ou des cartes PCMCIA permet de mettre à niveau la quantité de mémoire flash.

NVRAM: La mémoire vive rémanente (NVRAM) sert à stocker la configuration de démarrage. Dans certains équipements, la mémoire NVRAM est constituée de mémoires mortes reprogrammables électriquement EEPROM. Dans d'autres équipements, c'est une partition de la mémoire flash contenant le code de démarrage. Dans un cas comme dans l'autre, ces mémoires conservent leur contenu lors de la mise hors tension.

Bus: La plupart des routeurs comportent un bus système et un bus processeur. Le bus système est utilisé pour la communication entre le processeur et les interfaces et/ou les emplacements d'extension. Ce bus transfère les paquets vers et depuis les interfaces.

Le microprocesseur utilise le bus processeur pour accéder aux composants à partir du stockage du routeur. Ce bus transfère les instructions et les données vers ou depuis les adresses mémoire spécifiées.

ROM: La mémoire morte (ROM) sert à stocker de façon permanente le code de diagnostic de démarrage (ROM Monitor). La ROM a pour principales tâches d'exécuter des diagnostics matériels au cours du démarrage du routeur et de charger l'IOS de la mémoire flash vers la mémoire vive. Certains routeurs peuvent également contenir une version réduite de l'IOS qui peut être utilisée comme source de démarrage alternative. Les mémoires mortes ne sont pas effaçables. Elles ne peuvent être mises à niveau qu'en remplaçant les puces implantées dans les socles.

Interfaces: Les interfaces permettent au routeur de se connecter avec l'extérieur. Il possède trois types d'interfaces: LAN, WAN et Console/AUX. Les interfaces LAN sont en général des ports Ethernet ou Token Ring standard. Les puces de contrôleur de ces interfaces fournissent la logique de connexion du système au média. Les interfaces LAN peuvent être fixes ou modulaires.

Les interfaces WAN incluent des ports série, RNIS et une unité de transmission de données (CSU) intégrée. Comme les interfaces LAN, les interfaces WAN possèdent des puces de contrôleur spéciales pour les interfaces. Les interfaces WAN peuvent être fixes ou modulaires.

Les ports Console/AUX sont des ports série principalement utilisés pour la configuration initiale du routeur. Ce ne sont pas des ports réseau. Ils sont utilisés pour les sessions de terminal à partir des ports de communication de l'ordinateur ou via un modem.

Alimentation: L'alimentation fournit l'énergie nécessaire au fonctionnement des composants internes. Les grands routeurs peuvent être dotés d'alimentations multiples ou modulaires. Certains des petits routeurs sont dotés d'une alimentation externe.

Activité de média interactive

Glisser-Positionner : Composants internes des routeurs

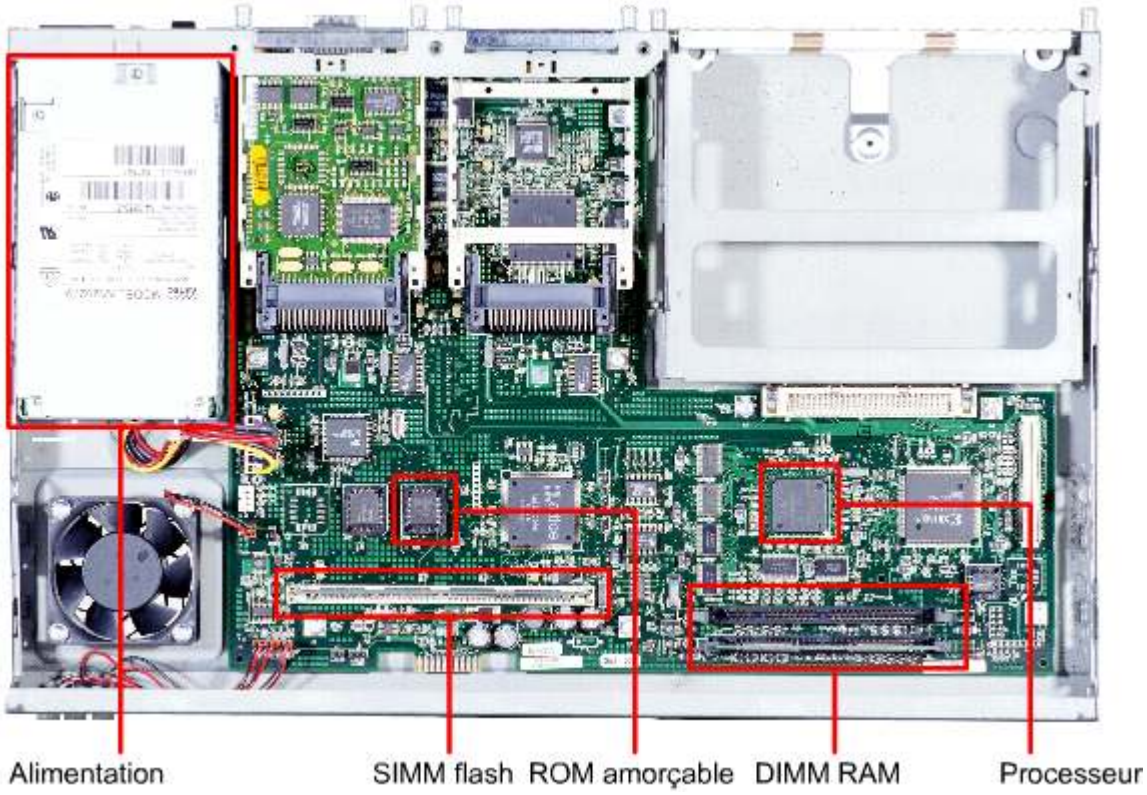
À la fin de cette activité, l'étudiant sera en mesure d'identifier les composants internes d'un routeur.

1.2 Routeurs

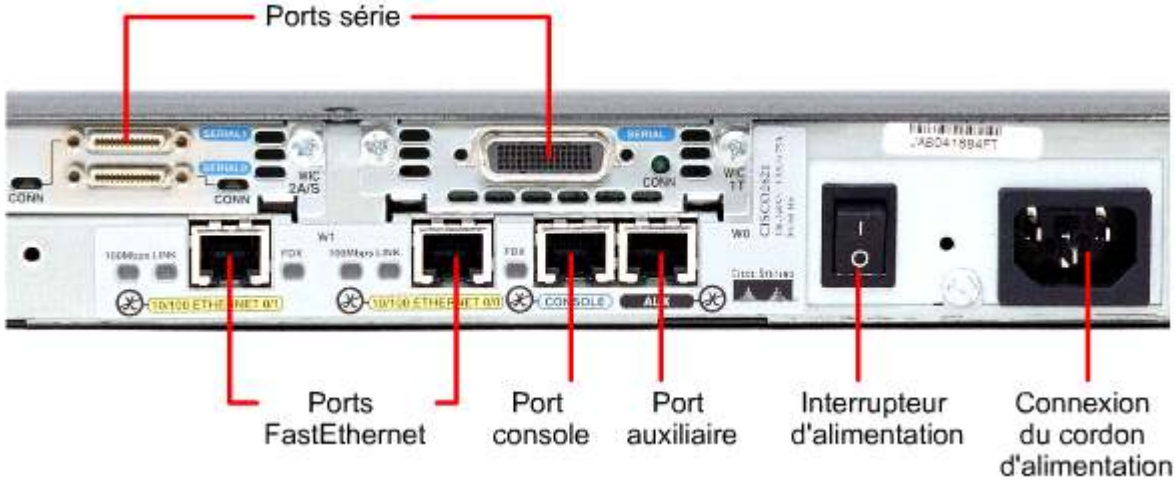
1.2.2 Caractéristiques physiques des routeurs

Il n'est pas essentiel de connaître l'emplacement des composants physiques internes d'un routeur pour savoir l'utiliser. Toutefois, dans certaines situations, telles que l'ajout de mémoire, cela peut s'avérer très utile.

Les composants proprement dits et leur emplacement varient selon les modèles. La figure 1 identifie les composants internes d'un routeur 2600.



La figure 2 présente certains des connecteurs externes d'un routeur 2600.



Activité de média interactive

Agrandissement : Routeur Cisco 1721

Dans cette vue agrandie, l'étudiant peut voir un routeur Cisco 1721.

Activité de média interactive

Agrandissement : Routeur Cisco 2621

Dans cette vue agrandie, l'étudiant peut voir un routeur Cisco 2621.

1.2 Routeurs

1.2.3 Connexions externes des routeurs

Les trois types de connexions de base d'un routeur sont les interfaces LAN, les interfaces WAN et les ports de gestion. Les interfaces LAN permettent au routeur de se connecter au média de réseau local. Il s'agit habituellement d'une forme d'Ethernet. Cependant, cela pourrait être d'autres technologies LAN comme Token Ring ou FDDI.

Les réseaux WAN fournissent des connexions à un site distant ou à l'Internet en utilisant les services d'un provider. Il peut s'agir de connexions série ou d'autres interfaces WAN. Avec certains types d'interfaces WAN, une unité externe, telle qu'une CSU, est nécessaire au niveau de la connexion locale du fournisseur d'accès. Dans d'autres cas, le routeur peut être connecté directement au réseau du fournisseur d'accès.

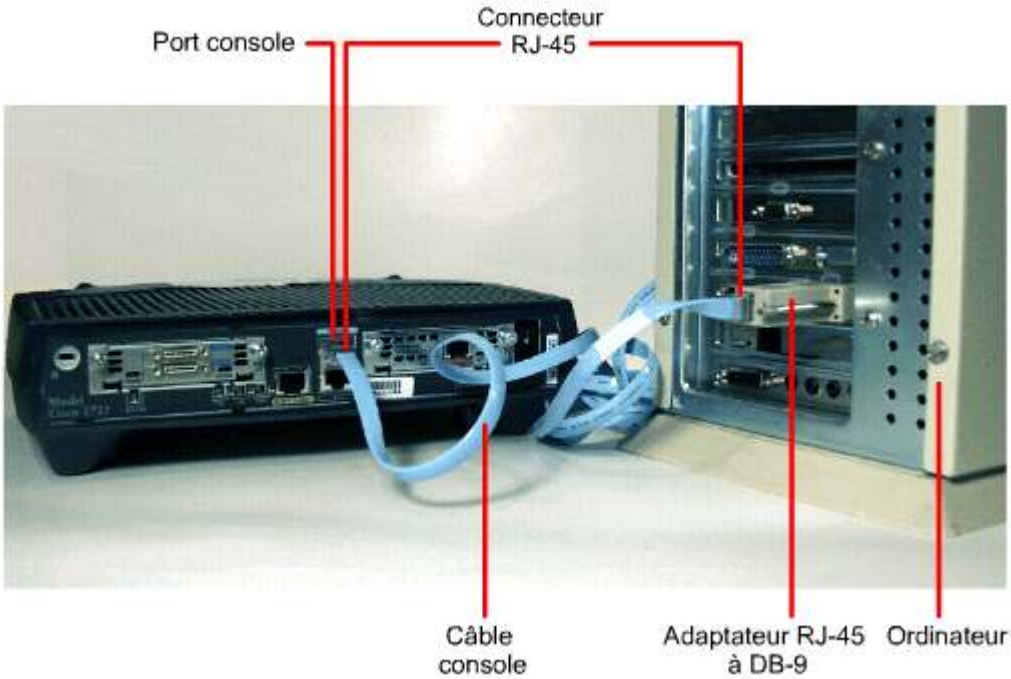
La fonction des ports de gestion est différente de celle des autres connexions. Les connexions LAN et WAN fournissent un réseau de liens à travers lesquels les paquets sont transmis. Le port de gestion fournit une connexion de type texte pour la configuration et le dépannage du routeur. Les interfaces de gestion communes sont les ports console et les ports auxiliaires. Ce sont des ports série asynchrones EIA-232. Ils sont connectés à un port de communications sur un ordinateur. L'ordinateur doit exécuter un programme d'émulation de terminal pour fournir une session texte avec le routeur. Cette session permet à l'administrateur du réseau de gérer le routeur (ou l'équipement).

1.2 Routeurs

1.2.4 Connexions des ports de gestion

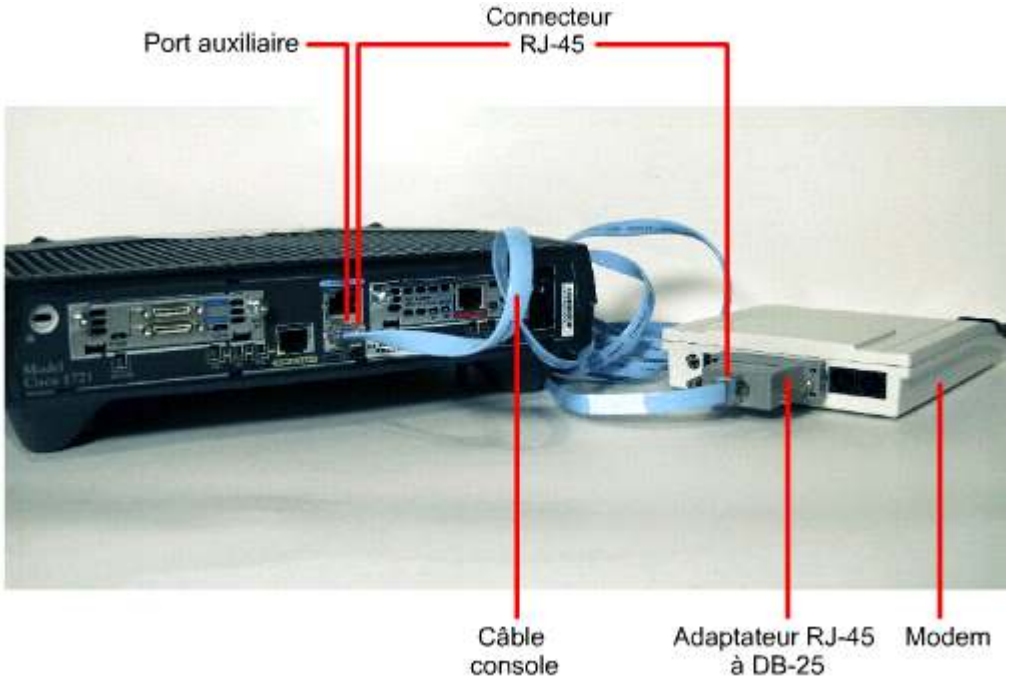
Le port console et le port auxiliaire (AUX) sont des ports de gestion. Ces ports série asynchrones ne sont pas conçus comme des ports de réseau. L'un de ces deux ports est nécessaire pour la configuration initiale du routeur. Le port console est recommandé pour cela. Les routeurs ne possèdent pas tous un port auxiliaire.

À la première mise en service du routeur, aucun paramètre de réseau n'est configuré. [1] Le routeur ne peut donc communiquer avec aucun réseau. Pour préparer le démarrage et la configuration initiale, connectez un terminal ASCII RS-232, ou un ordinateur émulant un terminal ASCII, au port console du système. Les commandes de configuration peuvent être alors entrées pour configurer le routeur.



Une fois que cette configuration initiale a été entrée dans le routeur via le port console ou le port auxiliaire, le routeur peut être connecté au réseau pour le dépannage ou la surveillance.

Le routeur peut aussi être configuré à distance en utilisant une session Telnet via un réseau IP ou en activant un modem connecté sur le port console ou le port auxiliaire du routeur. [2]

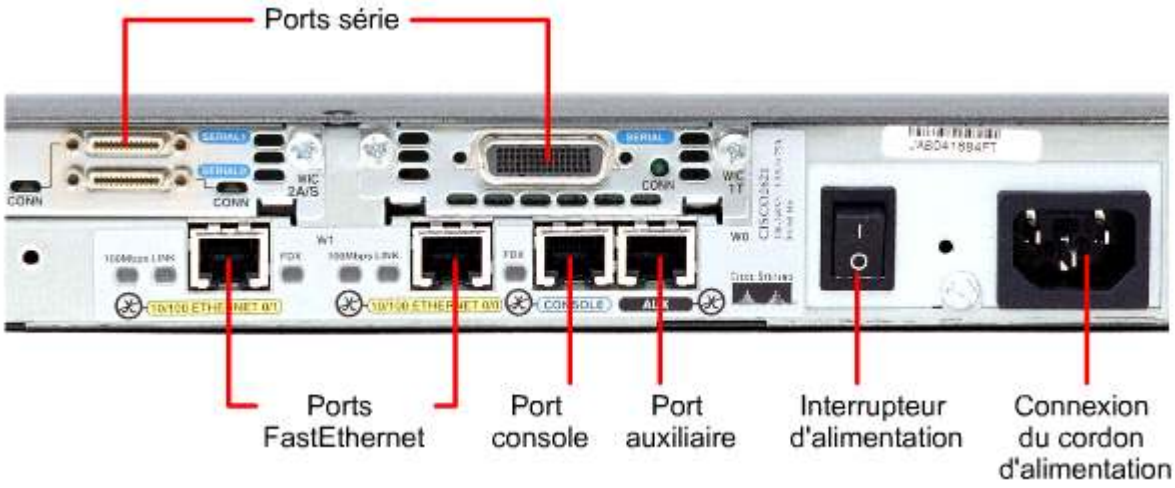


Pour le dépannage, il est également préférable d'utiliser le port console plutôt que le port auxiliaire, car il permet par défaut d'afficher les messages de démarrage, de débogage et les messages d'erreur du routeur. Le port console est également utilisable avant que les services réseau soient lancés ou lorsqu'ils sont défaillants. Par conséquent, le port console peut être utilisé pour les procédures de reprise après sinistre et de récupération de mots de passe.

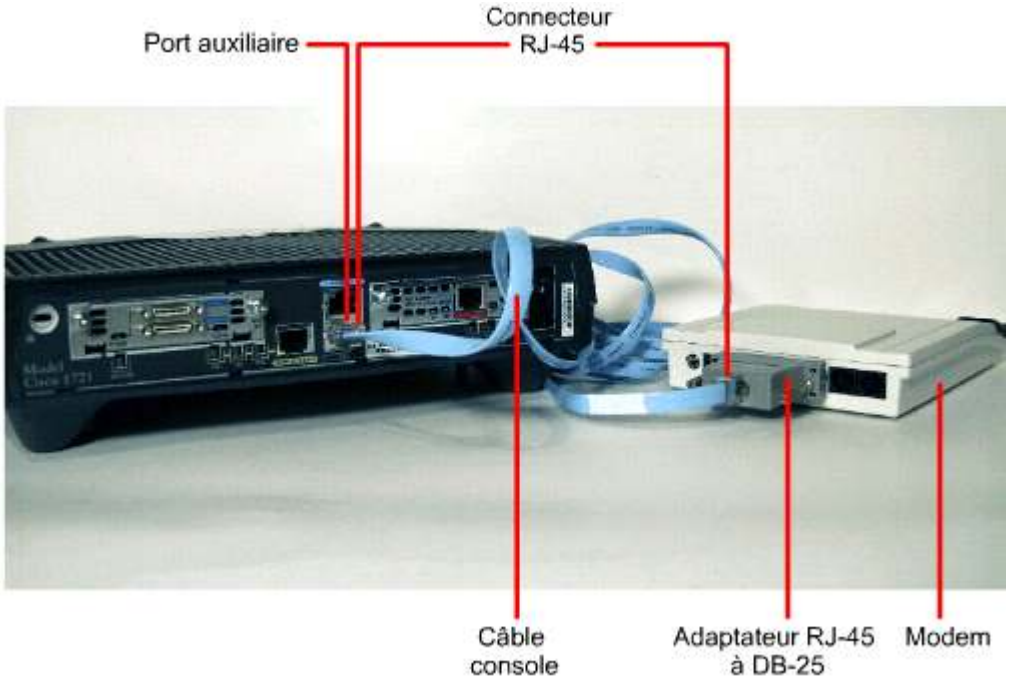
1.2 Routeurs

1.2.5 Connexion des interfaces en mode console

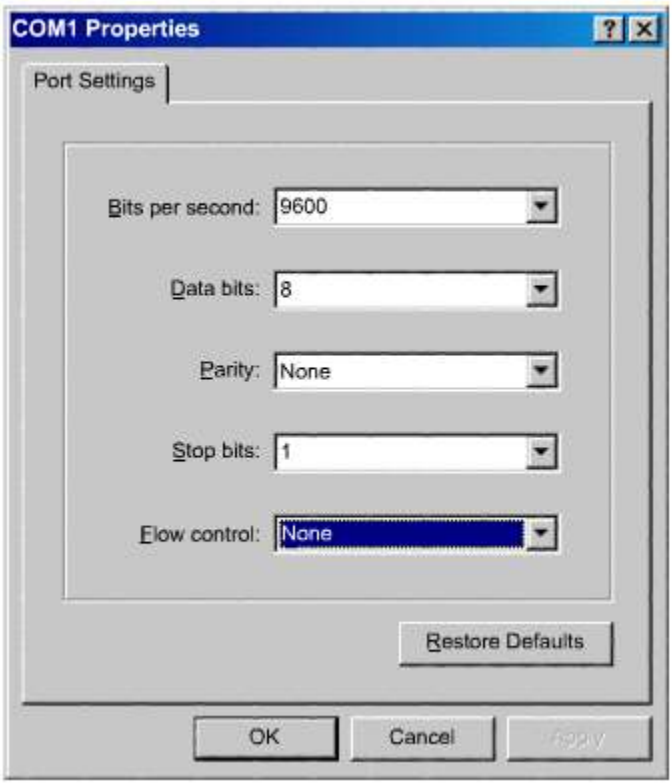
Le port console est un port de gestion qui fournit un accès hors bande au routeur. Il est utilisé pour la configuration initiale du routeur, pour la surveillance, et pour les procédures de reprise après sinistre. [1]



Un câble console ou câble à paires inversées et un adaptateur RJ-45 à DB-9 sont utilisés pour connecter le port console à un PC. [2] Cisco fournit l'adaptateur nécessaire pour se connecter au port console.



Le PC ou le terminal doit prendre en charge l'émulation de terminal VT100. Un logiciel d'émulation de terminal tel qu'HyperTerminal est habituellement utilisé.



Pour connecter le PC à un routeur:

1. Configurez le logiciel d'émulation de terminal sur le PC pour:
   - Le port com approprié
   - 9600 bauds
   - 8 bits de données
   - Aucune parité
   - 1 bit d'arrêt
   - Aucun contrôle de flux
2. Connectez le connecteur RJ-45 du câble à paires inversées au port console du routeur.

3. Connectez l'autre extrémité du câble à paires inversées à l'adaptateur RJ-45 à DB-9.
4. Connectez l'adaptateur DB-9 femelle à un PC.

Activité de TP

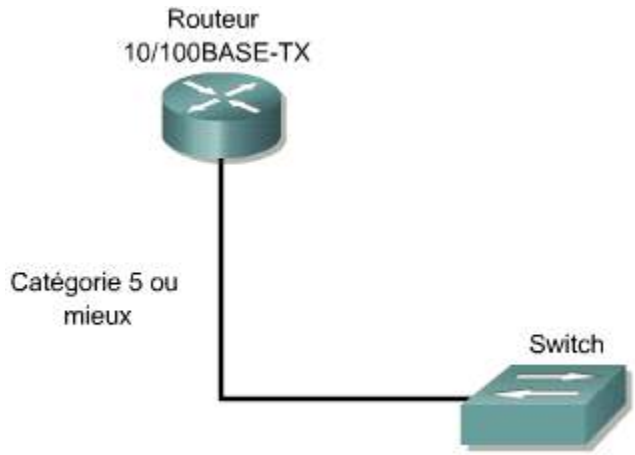
Exercice : Connexion des interfaces en mode console

L'objectif de ce TP est de connecter un PC à un routeur à l'aide d'un câble console ou à paires inversées.

1.2 Routeurs

1.2.6 Connexion des interfaces LAN

Dans la plupart des environnements LAN, le routeur est connecté au réseau à l'aide d'une interface Ethernet ou Fast Ethernet. Le routeur est un hôte qui communique avec le réseau LAN via un concentrateur ou un commutateur. Cette connexion doit être établie à l'aide d'un câble droit. Une interface de routeur 10/100BaseTX nécessite un câble à paires torsadées non blindée (UTP) de Catégorie 5 ou mieux, quel que soit le type du routeur. 1



Dans certains cas, la connexion Ethernet du routeur est reliée directement à l'ordinateur ou à un autre routeur. Ce type de connexion nécessite un câble croisé.

Vous devez utiliser l'interface correcte. Dans le cas contraire, le routeur et d'autres unités réseau peuvent être endommagées. De nombreux types différents de connexions utilisent le même style de connecteur. Par exemple les interfaces Ethernet, RNIS de base, Console, AUX, CSU/DSU intégré et Token Ring utilisent le même connecteur à huit broches, RJ-45, RJ-48 ou RJ-49.

Pour aider l'utilisateur, Cisco utilise un système de codes de couleurs pour identifier l'utilisation de chaque connecteur. La figure 2 présente certains des connecteurs externes d'un routeur 2600.

Port ou connexion	Type de port	Couleur	Connecté à	Câble
Ethernet	RJ-45	jaune	Concentrateur ou commutateur Ethernet	Droit
WAN T1/E1	RJ-48C/ CA81A	vert clair	Réseau T1 ou E1	RJ-48 T1
Console	8 broches	bleu clair	Port COM d'un ordinateur	Console (à paires inversées)
AUX	8 broches	noir	Modem	Console (à paires inversées)
BRI S/T	RJ-48C/ CA81A	orange	Unité NT1 ou PINX (Private Integrated Network eXchange)	RJ-48
BRI U WAN	RJ-49C/ CA11A	orange	Réseau RNIS	RJ-49
Token	UTP, STP	violet	Unité Token Ring	Token Ring RJ-45

Activité de TP

Exercice : Connexion des interfaces LAN d'un routeur

L'objectif de ce TP est d'identifier les interfaces Ethernet ou Fast Ethernet sur le routeur, puis de repérer les câbles appropriés pour connecter le routeur et le PC à un concentrateur ou à un commutateur.

Activité de média interactive

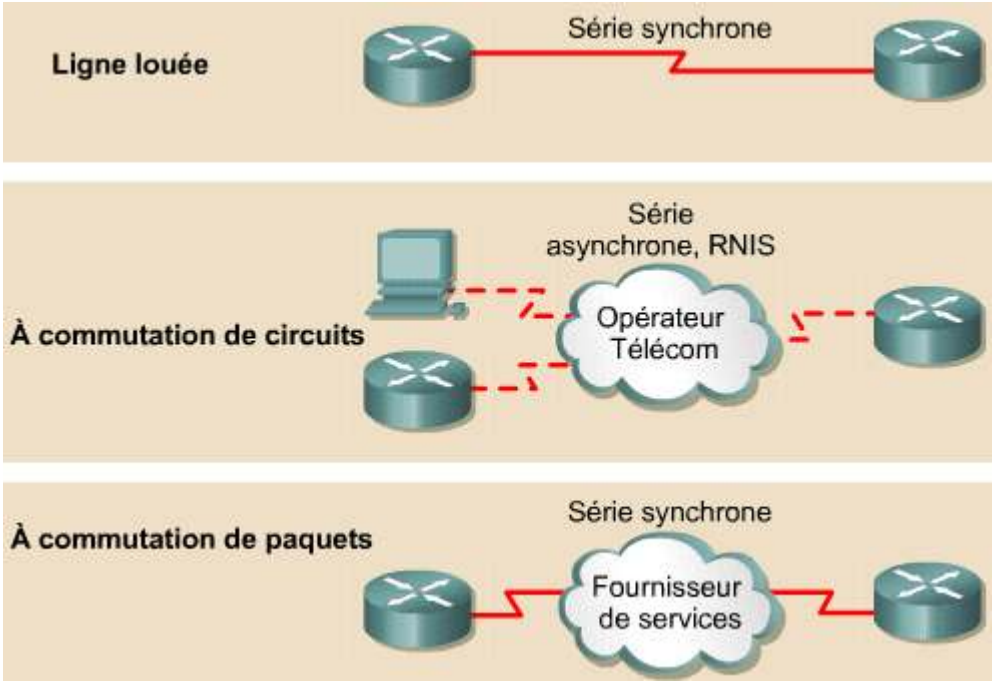
Glisser-Positionner : Connexion des interfaces LAN

À la fin de cette activité, l'étudiant sera en mesure d'identifier les composants et l'ordre approprié pour la connexion de l'interface Ethernet d'un commutateur au port AUI d'un routeur.

1.2 Routeurs

1.2.7 Connexion des interfaces WAN

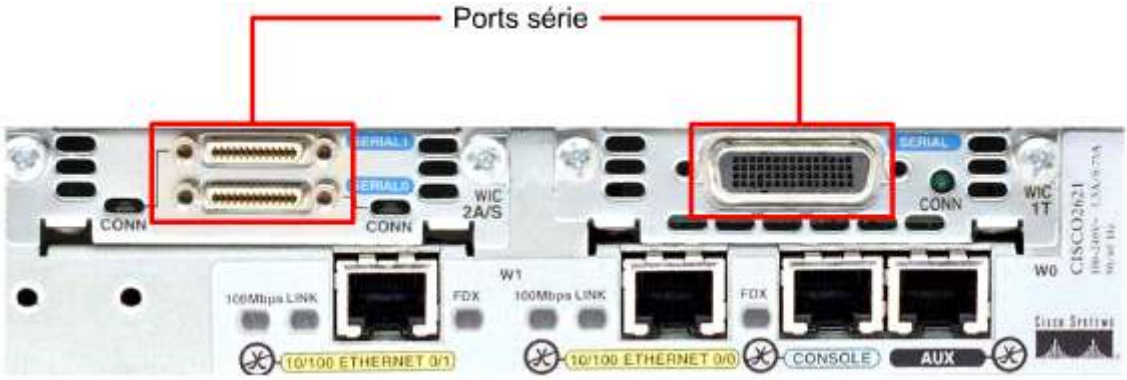
Les connexions WAN peuvent prendre des formes variées. Un WAN effectue des connexions de données à travers une zone géographique étendue en utilisant différents types de technologies. Ces services WAN sont habituellement loués à des fournisseurs de services. Ces types de connexions WAN sont notamment la ligne louée, la commutation de circuits et la commutation de paquets. 1



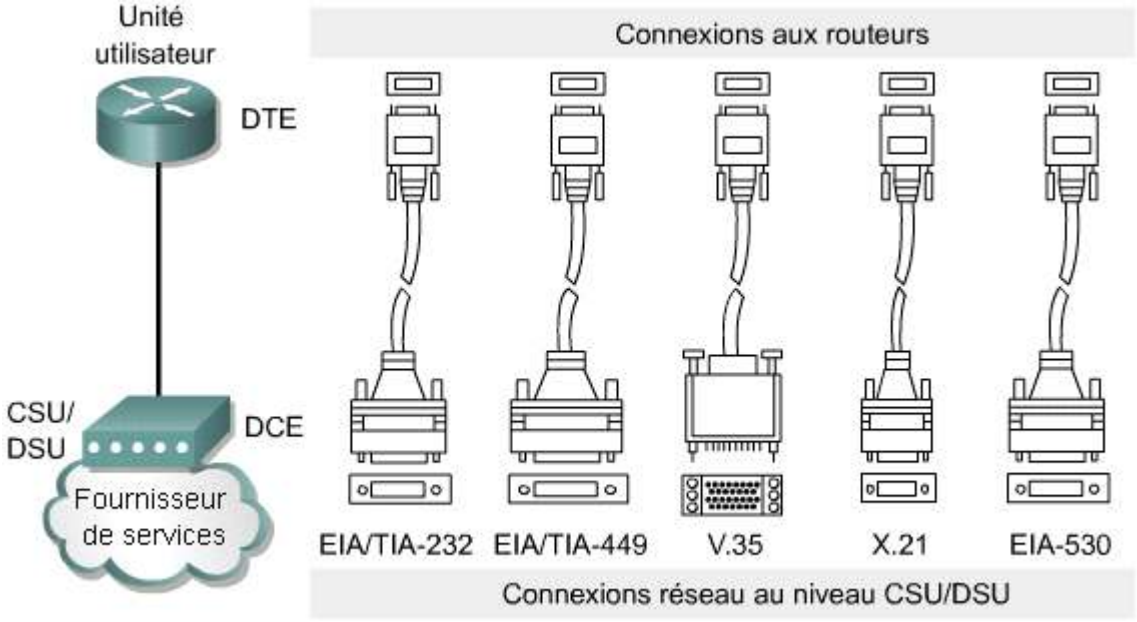
Pour chaque type de service WAN, l'équipement placé chez le client pour l'opérateur (CPE), souvent un routeur, est l'équipement terminal de traitement de données (ETTD). Celui-ci est connecté au fournisseur de services à l'aide d'un équipement de terminaison de circuit de données (ETCD), en général un modem ou une unité CSU/DSU. Cette unité est utilisée pour convertir les données de l'ETTD en un format acceptable pour le fournisseur de services WAN.

Les interfaces de routeur les plus couramment utilisées pour les services WAN sont sans doute les interfaces série. Il suffit pour sélectionner le câble série approprié de se poser ces quatre questions:

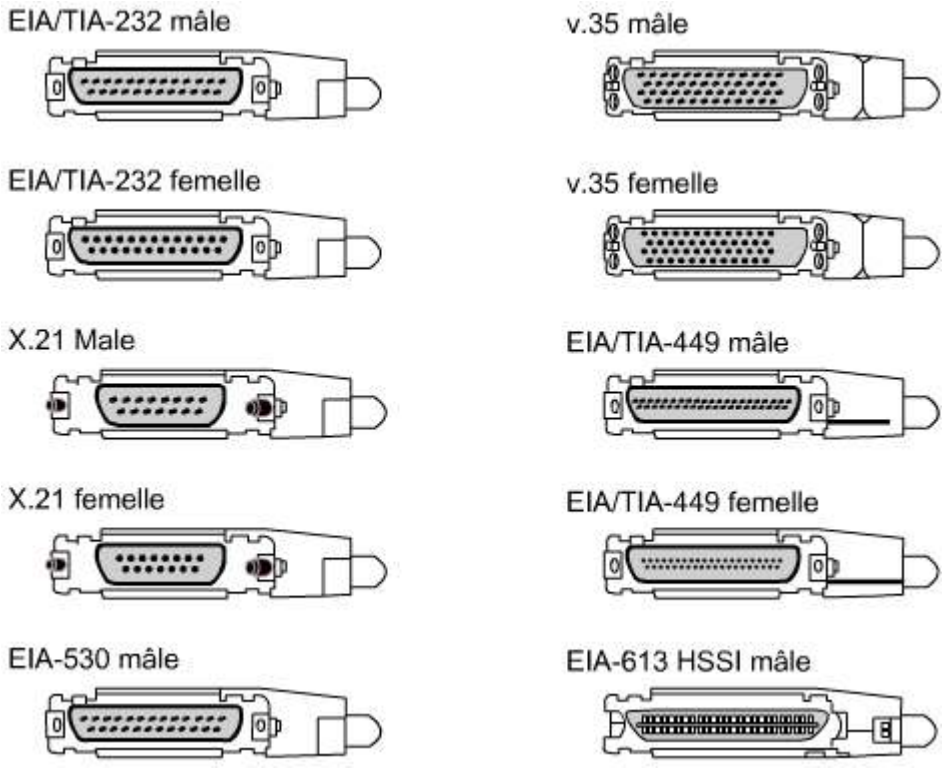
- Quel est le type de connexion vers le périphérique Cisco ? Les routeurs Cisco peuvent utiliser différents connecteurs pour les interfaces série. 2 L'interface de gauche est une interface série intelligente. Celle de droite est une connexion DB-60. La sélection du câble série qui relie le système réseau aux unités série est de ce fait une partie critique de la configuration d'un réseau WAN.



- Le système réseau est-il connecté à l'ETTD ou à l'ETCD ? ETTD et ETCD sont les deux types d'interfaces série que les équipements utilisent pour communiquer. La différence clé entre ces deux équipements est que l'ETCD fournit le signal d'horloge pour les communications sur le bus. La documentation de l'équipement doit spécifier s'il s'agit d'un ETTD ou d'un ETCD.
- Quelle norme de signalisation l'équipement nécessite-t-il? 3 Pour chaque équipement différent, une norme série différente peut être utilisée. Chaque norme définit les signaux sur le câble et spécifie le connecteur à l'extrémité du câble. La documentation de l'équipement devra toujours être consultée pour connaître la norme de signalisation.



- Un connecteur mâle ou femelle est-il nécessaire sur le câble? Si le connecteur comporte des broches, c'est un connecteur mâle. On reconnaît un connecteur femelle aux trous prévus pour recevoir les broches du connecteur mâle.



Activité de TP

Exercice : Connexion des interfaces WAN

L'objectif de ce TP est d'identifier les interfaces série sur le routeur et d'identifier et repérer les câbles appropriés pour interconnecter les routeurs.

Activité de média interactive

Glisser-Positionner : Connexion des interfaces WAN

À la fin de ce TP, l'étudiant sera en mesure d'identifier les composants et l'ordre de connexion de deux routeurs connectés via des interfaces série WAN.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Concepts relatifs aux réseaux WAN et aux réseaux LAN
- Rôle d'un routeur sur les réseaux WAN et des réseaux LAN
- Protocoles WAN
- Configuration de l'encapsulation
- Identification et description des composants internes d'un routeur
- Caractéristiques physiques d'un routeur
- Les ports communs d'un routeur
- Comment connecter les ports console, LAN et WAN d'un routeur

Résumé

- Un réseau WAN est un réseau de transmission de données qui couvre une vaste zone géographique.
- Un routeur est un ordinateur spécialisé conçu pour effectuer des fonctions spécifiques, différentes de celles d'un ordinateur de bureau.

Vue d'ensemble

La technologie Cisco est élaborée autour de la plate-forme logicielle Cisco IOS, c'est-à-dire le logiciel qui contrôle les fonctions de routage et de commutation des équipements réseau. L'administrateur réseau doit avoir une connaissance approfondie de l'IOS. Ce module présente une introduction aux notions fondamentales de l'IOS. Il permettra, par la pratique, d'examiner les fonctionnalités de ce système d'exploitation. Toutes les tâches de configuration réseau, des plus basiques aux plus complexes, nécessitent des bases solides en matière de configuration de routeur. Le présent module présente les outils et les techniques de configuration de routeur de base qui seront utilisées tout au long de ce cours.

À la fin de ce module, les étudiants doivent être en mesure de:

- Décrire l'objectif de l'IOS
- Décrire le fonctionnement de base de l'IOS
- Identifier les diverses fonctionnalités de l'IOS
- Identifier les méthodes permettant d'établir une session d'interface de commande en ligne (CLI) avec le routeur
- Basculer entre les modes d'exécution des commandes (EXEC) et le mode privilégié
- Établir une session HyperTerminal sur un routeur
- Se connecter à un routeur
- Utiliser la fonction d'aide de l'interface de commande en ligne
- Résoudre les erreurs au niveau des commandes

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
2.1	Utilisation de la plate-forme logicielle Cisco IOS
2.2	Démarrage d'un routeur

Ce module porte sur les objectifs suivants de l'examen de certificationCCNA 640-801 :

Planification et conception	Mise en œuvre et	Dépannage	Technologie
	• Mise en œuvre d'un LAN • Gestion des fichiers de configuration des équipements et de l'image système	• Dépannage d'un équipement dans un réseau en fonctionnement	• Description des composants d'équipements réseau

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception ou modification d'un LAN simple à l'aide de produits Cisco	• Mise en œuvre d'un LAN	• Dépannage d'un équipement dans un réseau en fonctionnement	

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
	• Établissement de communication entre un équipement terminal et l'IOS du routeur, et utilisation de l'IOS en vue de l'analyse du système • Création d'une configuration initiale sur un routeur et enregistrement du fichier de configuration obtenu • Description et installation du matériel et du logiciel requis pour pouvoir communiquer via un réseau	• Description du matériel et du logiciel requis pour pouvoir communiquer via un réseau • Description du rôle et du fonctionnement de base de la plate-forme logicielle Cisco IOS • Identification des principaux composants internes et externes d'un routeur, et description des fonctionnalités associées • Identification et descrip-tion des étapes de la sequ-ence d'amorçage d'un routeur

2.1 Utilisation de la plate-forme logicielle Cisco IOS

2.1.1 L'objectif de la plate-forme logicielle Cisco IOS

À l'instar d'un ordinateur, un routeur ou un commutateur ne peut pas fonctionner sans système d'exploitation. Cisco a nommé son système d'exploitation Cisco Internetwork Operating System ou Cisco IOS. C'est l'architecture logicielle qui est incorporée dans tous les routeurs Cisco et qui constitue également le système d'exploitation des commutateurs Catalyst. Sans système d'exploitation, le matériel est inopérant. L'IOS fournit les services réseau suivants:

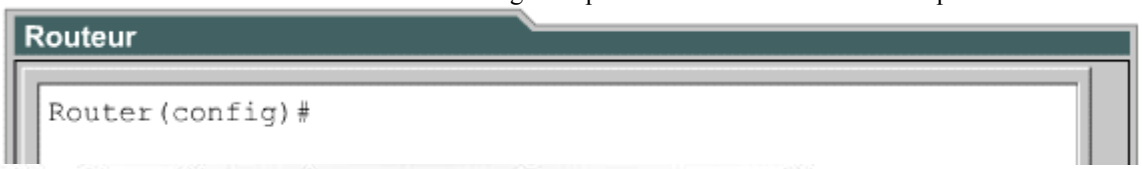
- fonctions de routage et de commutation de base,
- accès fiable et sécurisé aux ressources en réseau,
- évolutivité du réseau.

2.1 Utilisation de la plate-forme logicielle Cisco IOS

2.1.2 Interface utilisateur de routeur

L'IOS utilise une interface de commande en ligne (CLI) comme environnement de console traditionnel. L'IOS est une technologie centrale qui s'étend à pratiquement tous les produits Cisco. Son fonctionnement peut varier suivant les unités d'interconnexion de réseaux sur lesquelles il est utilisé.

Cet environnement est accessible de différentes façons. La session en mode console permet d'accéder à l'interface de commande en ligne. La console se connecte alors directement à la connexion de console du routeur à partir d'un ordinateur ou d'un terminal, via une liaison série basse vitesse. L'autre façon d'accéder à l'interface de commande en ligne CLI consiste à utiliser une connexion à accès commuté au moyen d'un modem ou d'un null modem connecté au port AUX du routeur. Aucune de ces méthodes ne nécessite la configuration de services réseau sur le routeur. Une autre méthode consiste à établir une connexion Telnet avec le routeur. Pour cela, au moins une interface doit être configurée avec une adresse IP, et des sessions de terminal virtuelles doivent être configurées pour la connexion et les mots de passe.



L'interface utilisateur d'un routeur ou d'un commutateur utilise un programme de terminal ASCII. La version la plus utilisée est le programme Windows HyperTerminal.

2.1 Utilisation de la plate-forme logicielle Cisco IOS

2.1.3 Modes d'interface utilisateur des routeurs

L'interface de commande en ligne (CLI) utilise une structure hiérarchique. Selon les tâches que l'utilisateur souhaite accomplir, cette structure nécessite l'entrée en différents modes. Par exemple, pour configurer une interface de routeur, l'utilisateur doit passer en mode de configuration d'interface. Dans ce mode, toutes les configurations entrées s'appliquent à cette interface particulière. Chaque mode de configuration est signalé par une invite distinctive et n'autorise que les commandes appropriées pour ce mode.

L'IOS fournit un service d'interpréteur de commande baptisé programme d'exécution des commandes (EXEC). À chaque entrée de commande, le programme d'exécution valide puis exécute la commande.

Par mesure de sécurité, l'IOS sépare les sessions d'exécution en deux niveaux d'accès. Ces niveaux sont le mode utilisateur et le mode privilégié. Le mode privilégié est également appelé mode enable. Voici les caractéristiques du mode utilisateur et du mode privilégié :

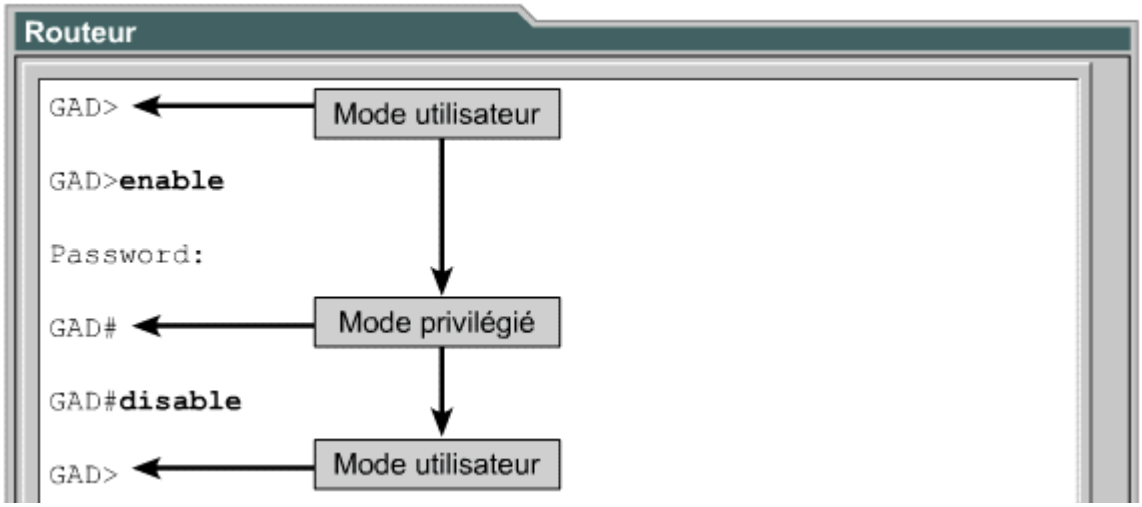
- Le mode utilisateur n'autorise qu'un nombre limité de commandes de surveillance de base. C'est ce que l'on appelle un mode de « visualisation seule ». Le niveau utilisateur n'autorise aucune commande susceptible de modifier la configuration du routeur. Le mode utilisateur est identifié par l'invite >. 1

Mode EXEC	Invite	Utilisation type
Utilisateur	GAD>	vérification de l'état du routeur
Privilégié	GAD#	accès aux modes de

- Le mode privilégié accède à toutes les commandes du routeur. Ce mode peut être configuré pour demander à l'utilisateur d'indiquer un mot de passe pour pouvoir y accéder. Pour une protection renforcée, il peut également être configuré pour demander une ID utilisateur. Ainsi, seuls les utilisateurs autorisés peuvent accéder au routeur. Les commandes de configuration et de gestion exigent que l'administrateur réseau soit au niveau privilégié. Le mode de configuration globale et les autres modes de configuration plus spécifiques ne peuvent être activés qu'à partir du mode privilégié. Le mode privilégié peut être identifié par l'invite #.

Pour accéder au niveau privilégié depuis le niveau utilisateur, entrez la commande **enable** à l'invite >. 2 Si un mot de passe est configuré, le routeur le demande. Pour des raisons de sécurité, les équipements de réseau Cisco n'affichent pas le mot de

passe entré. Lorsque le mot de passe correct est entré, l'invite du routeur se change en #, indiquant que l'utilisateur se trouve maintenant en mode privilégié. L'entrée d'un point d'interrogation (**?**) au niveau privilégié entraîne l'affichage de davantage d'options de commande qu'au niveau utilisateur.



Activité de TP

Activité en ligne : Connexion au routeur

L'objectif de ce TP est d'accéder à l'interface de commande en ligne du routeur et d'activer les options de configuration du niveau privilégié.

Activité de TP

Activité en ligne : Modes d'interface utilisateur d'un routeur

Dans ce TP, les étudiants vont apprendre à utiliser la commande enable pour passer en mode privilégié dans l'IOS.

2.1 Utilisation de la plate-forme logicielle Cisco IOS

2.1.4 Caractéristiques de la plate-forme logicielle Cisco IOS

Cisco fournit des images IOS pour une vaste gamme de plates-formes de produits de réseau.

Afin d'optimiser la plate-forme logicielle Cisco IOS pour ces différentes plates-formes, Cisco développe différentes images IOS. Chaque image représente un jeu de fonctions adapté aux différentes plates-formes, aux ressources mémoire disponibles, ainsi qu'aux besoins du client.

Bien qu'il existe différentes IOS pour les différents modèles d'équipements et les jeux de fonctions de Cisco, la structure de commande de configuration de base reste identique. Les compétences en configuration et en dépannage acquises sur n'importe quel équipement s'appliquent à une vaste gamme de produits.

La convention d'attribution de noms des différentes versions de l'IOS comprend trois parties : 1

Le nom comporte trois parties séparées par un tiret (par exemple, xxxx-yyyy-ww) :
- xxxx = plate-forme
- yyyy = fonctions
- ww = Format - emplacement d'exécution si compressé

Codes de nom	
Plate-forme (matériel) (liste partielle)	
c1005	1005
c1600	1600
c1700	1700, 1720, 1750
c2500	25xx, 3xxx, 5100, AO (11.2 and later only)
c2600	2600
c2800	Catalyst 2800
c2900	2910, 2950
c3620	3620
c3640	3640
c4000	4000 (11.2 and later only)
c4500	4500, 4700
Fonctions (liste partielle)	
b	Appletalk
boot	boot image
c	CommServer lite (CiscoPro)
drag	IOS based diagnostic images
g	ISDN subset (SNMP, IP, Bridging, ISDN, PPP, IPX, Atalk)
i	IP subset (SNMP, IP, Bridging, WAN, Remote Node, Terminal Services)
n	IPX
q	Async
t	Telco return (12.0)
y	reduced IP (SNMP, IP RIP/IGRP/EIGRP, Bridging, ISDN, PPP) (C1003/4)
z	managed modems
40	40 bit encryption
56	56 bit encryption
Format (emplacement d'exécution de l'image dans le routeur)	
f	flash
m	ram
r	rom
l	relocatable
Types de compression	
z	zip compressed (note lower case)
x	m zip compressed
w	"STAC" compressed

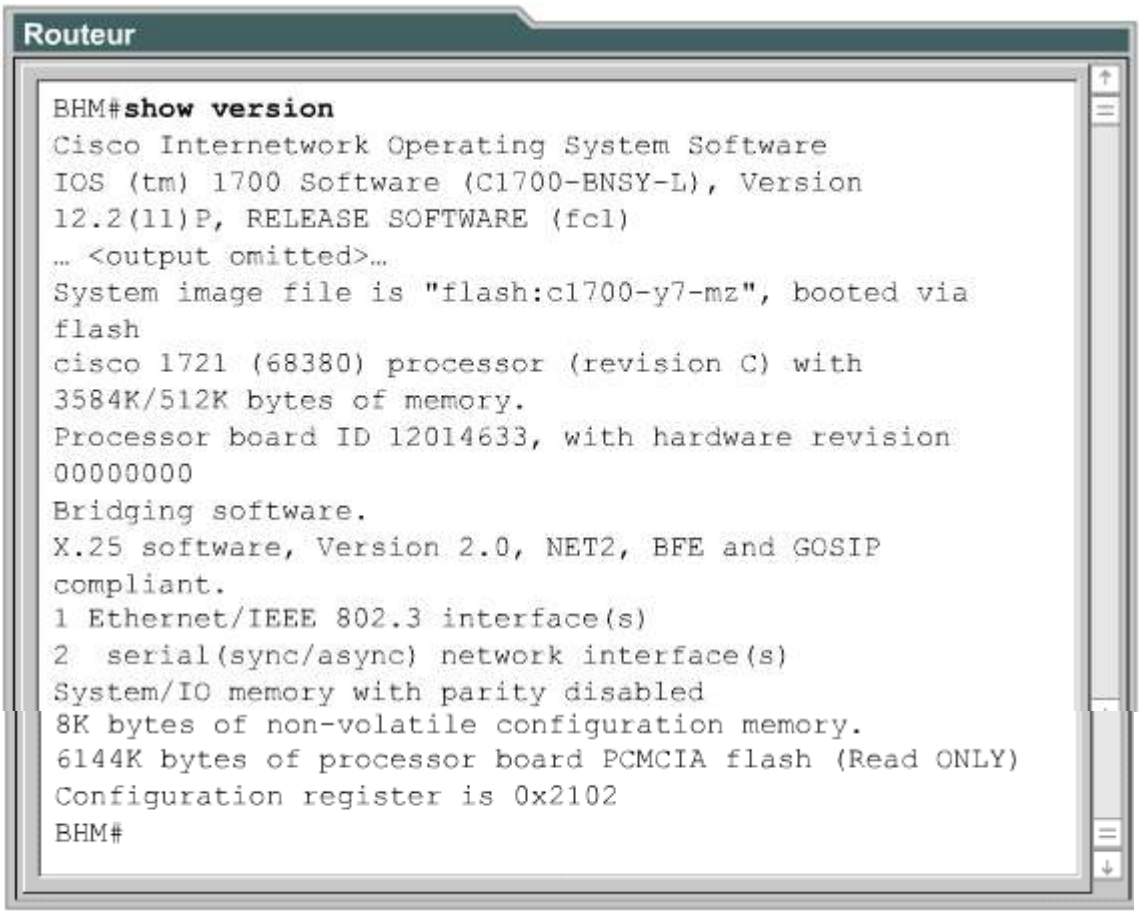
- la plate-forme sur laquelle l'image est exécutée,
- les fonctions spéciales prises en charge dans l'image,
- l'endroit où l'image s'exécute avec un indicateur précisant si elle est zippée ou comprimée.

Il est possible de sélectionner des fonctions spécifiques de l'IOS à l'aide de Cisco Software Advisor. Cisco Software Advisor est un outil interactif qui fournit les informations les plus à jour et permet de sélectionner des options qui répondent aux exigences du réseau.

L'un des points essentiels dont il faut tenir compte lors de la sélection d'une nouvelle image IOS est sa compatibilité avec la mémoire flash et la mémoire RAM. En général, plus la version est récente et plus elle fournit de fonctionnalités, et plus elle requiert de mémoire. Utilisez la commande **`show version`** sur l'équipement Cisco pour vérifier l'image en cours et la

mémoire flash disponible. Le site de support Cisco propose des outils qui permettent de déterminer les quantités de mémoire flash et de mémoire vive nécessaires pour chaque image.

Avant d'installer une nouvelle image IOS sur le routeur, vérifiez si ce dernier répond aux besoins en mémoire pour cette image. Pour connaître la quantité de mémoire RAM, exécutez la commande **`show version`**: 2




```
... <output omitted> ... cisco 1721 (68380) processor (revision C) with 3584K/512K
bytes of memory.
```

Cette ligne indique quelle quantité de mémoire principale et de mémoire partagée est installée dans le routeur. Certaines plates-formes utilisent une partie de la mémoire DRAM comme mémoire partagée. Cela est pris en compte dans les besoins en mémoire, aussi les deux valeurs doivent-elles être ajoutées pour connaître la quantité de mémoire DRAM installée dans le routeur.

Pour trouver la quantité de mémoire flash, exécutez la commande **`show flash`** :

```
GAD#show flash
... <output omitted> ...
15998976 bytes total (10889728 bytes free)
```

2.1 Utilisation de la plate-forme logicielle Cisco IOS

2.1.5 Fonctionnement de la plate-forme logicielle Cisco IOS

Les équipements Cisco ISO possèdent trois environnements d'exploitation ou modes distincts: 1

- Moniteur ROM
- Mémoire ROM amorçable
- Cisco IOS

Environnement d'exploitation	Invite	Utilisation
Moniteur ROM	> or ROMMON>	Panne ou récupération de mot de passe
ROM amorçable	Router(boot)>	Mise à niveau d'image flash
Plate-forme logicielle Cisco IOS	Router>	Fonctionnement normal

Le processus de démarrage du routeur se charge normalement en mémoire RAM et exécute l'un de ces environnements d'exploitation. L'administrateur système peut paramétrer le registre de configuration pour contrôler le mode de démarrage par défaut du routeur.

Le moniteur ROM exécute le processus de bootstrap et fournit des fonctions et des diagnostics de bas niveau. Il sert au redémarrage suite à une panne système et à la récupération des mots de passe perdus. Aucune interface réseau ne permet d'accéder au moniteur ROM. Il n'est accessible qu'au moyen d'une connexion physique directe à travers le port console.

Lorsque le routeur fonctionne en mode ROM amorçable, seul un sous-ensemble limité des fonctions de l'IOS est disponible. La mémoire ROM amorçable permet les opérations d'écriture en mémoire flash et est principalement utilisée pour remplacer l'image IOS qui est stockée en mémoire flash. L'image IOS peut être modifiée en ROM amorçable en utilisant la commande **`copy tftp flash`**, qui copie une image IOS stockée sur un serveur TFTP dans la mémoire flash du routeur.

Pour fonctionner normalement, un routeur requiert l'utilisation de l'image IOS complète qui est stockée dans la mémoire flash. Sur certains équipements, l'IOS est directement exécuté à partir de la mémoire flash. Cependant, certains routeurs Cisco requièrent le chargement d'une copie de l'IOS dans la mémoire RAM et son exécution à partir de celle-ci. Certaines images IOS sont stockées en mémoire flash dans un format comprimé et doivent être décompressées lors de la copie vers la mémoire RAM.

Pour voir l'image et la version de l'IOS qui s'exécute, utilisez la commande **`show version`**, qui indique également le paramètre du registre de configuration. La commande **`show flash`** permet de vérifier que le système dispose de suffisamment de mémoire pour charger une nouvelle image IOS. 2

Routeur

```
BHM#show flash
PCMCIA flash directory:
File  Length    Name/status
  1   6007232   c1700-bnsy-l.212-11.p
[6007296 bytes used, 284160 available, 6291456
total]
6144K bytes of processor board PCMCIA flash (Read
ONLY)
BHM#
```

Activité de TP

Activité en ligne : Fonctionnement de l'IOS

Ce TP explique comment placer une nouvelle image IOS sur le routeur.

2.2 Démarrage d'un routeur

2.2.1 Démarrage initial des routeurs Cisco

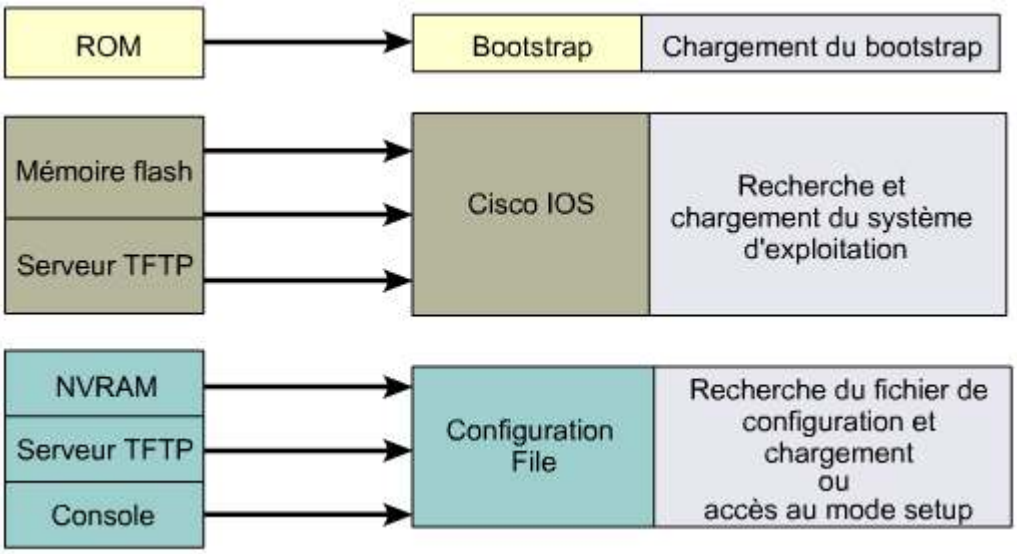
Pour démarrer, un routeur doit charger le bootstrap et le système d'exploitation, ainsi qu'un fichier de configuration. S'il ne trouve pas le fichier de configuration, le routeur passe en mode setup. À la fin du mode setup, une copie de sauvegarde du fichier de configuration peut être enregistrée en mémoire vive rémanente (NVRAM).

L'objectif des routines de démarrage de la plate-forme logicielle Cisco IOS est de lancer les opérations de routage. Pour ce faire, les routines de démarrage effectuent les opérations suivantes:

- vérifier que le matériel de routeur a été testé et est opérationnel,
- trouver et charger l'IOS,
- trouver et appliquer le fichier de configuration de démarrage ou passer en mode setup.

Lorsque vous mettez un routeur Cisco sous tension, il effectue un test automatique de mise sous tension (POST). Au cours de ce test, il exécute les diagnostics chargés en mémoire ROM sur tous les modules physiques. Ces diagnostics vérifient le fonctionnement de base du processeur, de la mémoire et des ports d'interface réseau. Une fois le matériel vérifié, le routeur initialise le logiciel.

Après le test POST, l'initialisation du routeur se déroule comme suit: 1



Étape 1 Le chargeur de bootstrap générique de la mémoire ROM s'exécute. Un bootstrap est un jeu d'instructions simple qui teste le matériel et initialise l'IOS.

Étape 2 L'IOS peut se trouver à différents endroits. Le champ de démarrage du registre de configuration détermine l'endroit à utiliser au moment du chargement de l'IOS. Si le champ indique un chargement à partir de la mémoire flash ou du réseau, les commandes boot system du fichier de configuration précisent le nom et l'emplacement exact de l'image.

Étape 3 L'image du système d'exploitation est chargée. Lorsque l'IOS est chargé et opérationnel, une liste des composants matériels et logiciels s'affiche sur l'écran de la console.

Étape 4 Le fichier de configuration stocké dans la mémoire NVRAM est chargé dans la mémoire principale, puis il est exécuté ligne par ligne. Les commandes de configuration lancent les processus de routage, fournissent les adresses aux interfaces et définissent les autres caractéristiques de fonctionnement du routeur.

Étape 5 Si la mémoire NVRAM ne contient pas de fichier de configuration valide, le système d'exploitation recherche un serveur TFTP disponible. S'il n'en trouve aucun, le dialogue de configuration est établi.

Le mode setup n'est pas conçu pour entrer des fonctions de protocole complexes dans le routeur. Sa principale fonction et de permettre à l'administrateur d'installer une configuration minimale pour un routeur s'il lui est impossible d'obtenir une configuration d'une autre source.

Dans le mode setup, les réponses par défaut apparaissent entre crochets **[ ]** à la suite de la question. 2Appuyez sur la touche **Entrée** pour accepter les valeurs par défaut. Au cours du processus de configuration, vous pouvez appuyer sur **Ctrl-C** à tout moment pour mettre fin au processus. Lorsque vous achevez la configuration à l'aide de **Ctrl-C**, toutes les interfaces sont administrativement désactivées.

Routeur

```
#setup

--System Configuration Dialog--
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Continue with configuration dialog? [yes].

First, would you like to see the current interface summary?
[yes]

Interface    IP-Address    OK?   Method    Status   Protocol
TokenRing0   unassigned    NO    not set    down     down
Ethernet0    unassigned    NO    not set    down     down
Serial0      unassigned    NO    not set    down     down
Fddi0        unassigned    NO    not set    down     down
```

Activité de TP

Exercice : Configuration d'un routeur à l'aide de setup

Au cours de ce TP, les étudiants vont utiliser le dialogue de configuration du système (setup) pour établir la configuration de base d'un routeur.

Une fois le processus de configuration en mode setup terminé, les options suivantes s'affichent :

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]:
```

2.2 Démarrage d'un routeur

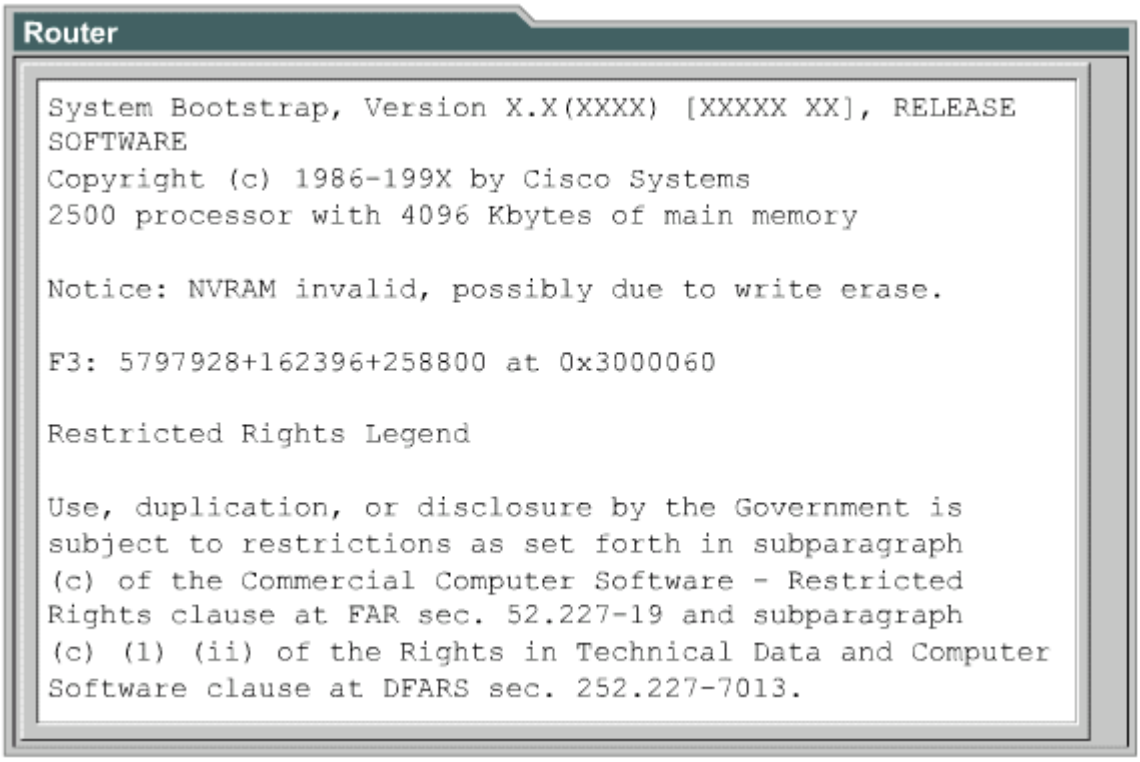
2.2.2 Indicateurs LED de routeur

Les routeurs Cisco utilisent des indicateurs LED pour fournir des informations de statut. Ces LED sont différentes selon le modèle de routeur Cisco.

Une LED d'interface indique l'activité de l'interface correspondante. Si une LED est éteinte alors que l'interface est active et correctement connectée, il peut y avoir un problème. Si une interface est occupée en permanence, sa LED reste toujours allumée. La LED OK de couleur verte située à droite du port AUX s'allume lorsque le système s'initialise correctement. 1

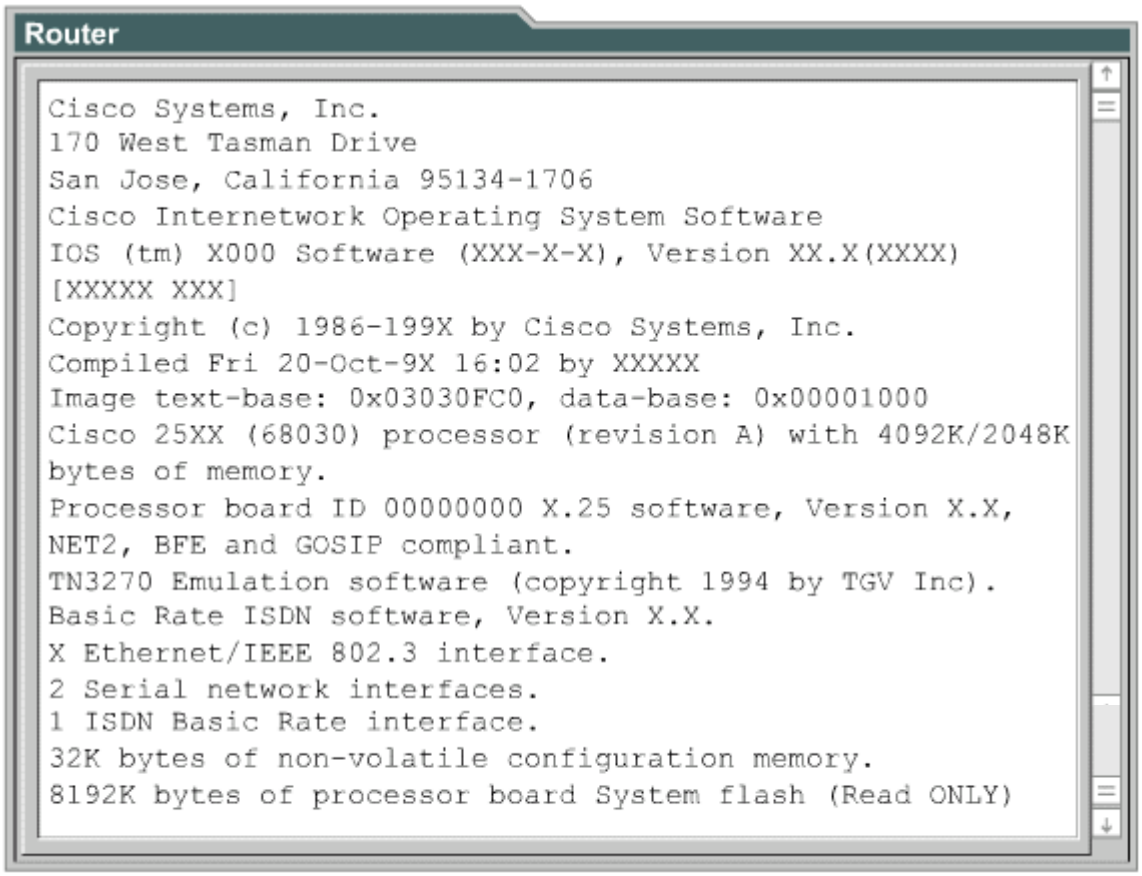
2.2.3 Examen du démarrage initial d'un routeur

Les exemples des figures 1 à 3 illustrent les informations et les messages qui s'affichent au cours du démarrage initial. Ces informations varient selon les interfaces du routeur et la version de l'IOS. Les écrans représentés dans ce graphique sont fournis pour référence uniquement et peuvent ne pas correspondre exactement à ceux de la console.



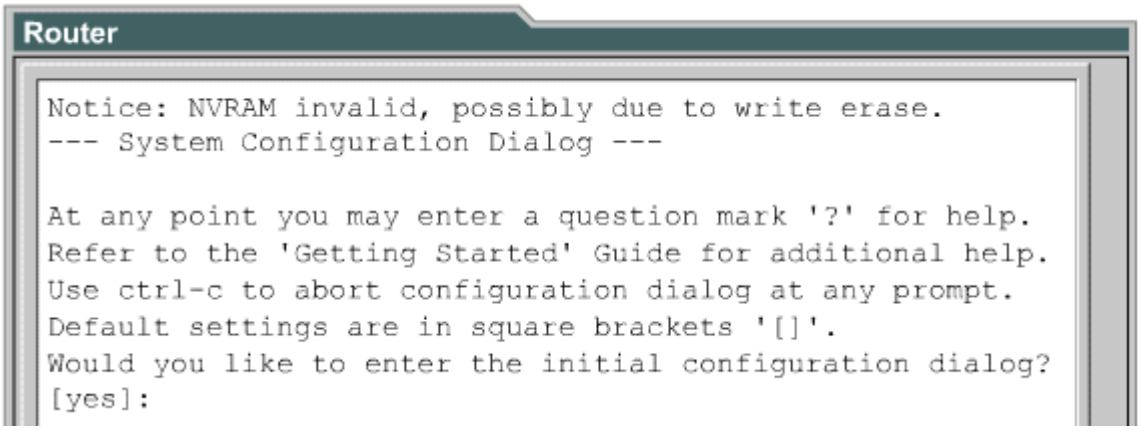
Dans la Figure 1, le message "NVRAM invalid, possibly due to write erase", indique à l'utilisateur que ce routeur n'a pas encore été configuré ou que la mémoire NVRAM a été effacée. Il faut enregistrer le fichier de configuration dans la mémoire NVRAM du routeur, puis configurer le routeur pour qu'il utilise ce fichier. La valeur configurée en usine pour le registre de configuration est 0x2102, ce qui indique que le routeur doit tenter de charger une image IOS à partir de la mémoire flash.

Dans la Figure 2, l'utilisateur peut déterminer la version bootstrap et la version de l'IOS que le routeur utilise ainsi que le modèle de routeur, le processeur et la quantité de mémoire dont dispose le routeur. Ce graphique contient également les informations suivantes:



- le nombre d'interfaces,
- les types d'interfaces,
- la quantité de mémoire NVRAM,
- la quantité de mémoire flash.

Dans la figure 3, on voit que l'utilisateur a la possibilité de passer en mode setup. Rappelez-vous que ce mode a pour but de permettre à l'administrateur d'installer une configuration minimale pour un routeur, s'il est impossible d'obtenir une configuration d'une autre source.



2.2 Démarrage d'un routeur

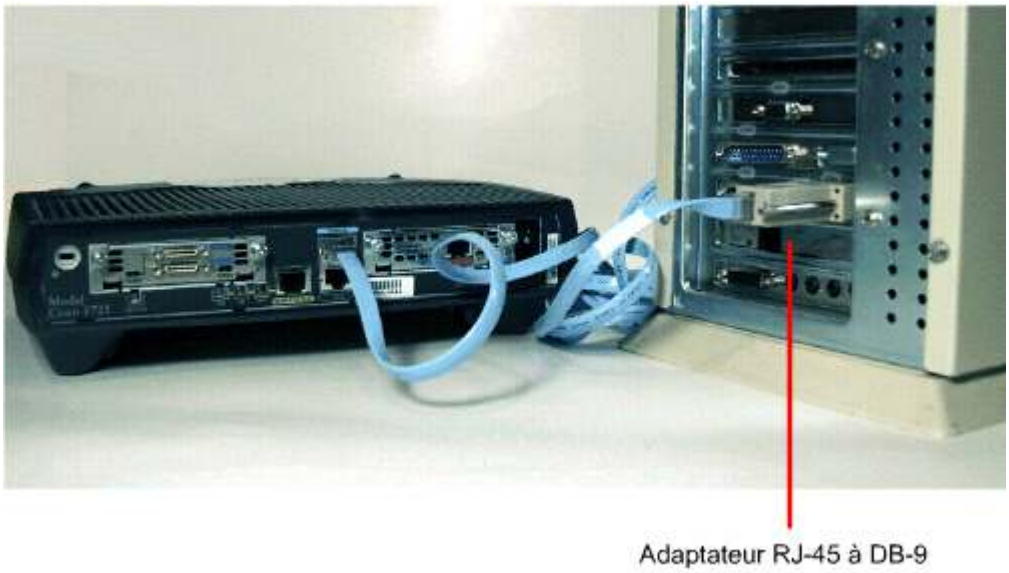
2.2.4 Établissement d'une session HyperTerminal

Tous les routeurs Cisco sont dotés d'un port console série asynchrone TIA/EIA-232 (RJ-45). Des câbles et des adaptateurs sont nécessaires pour connecter un terminal de console au port console. Un terminal de console est un terminal ASCII ou un PC exécutant un logiciel d'émulation de terminal tel qu'HyperTerminal. Pour connecter un PC exécutant un logiciel d'émulation de terminal au port console, utilisez le câble à paires inversées RJ-45 à RJ-45 avec l'adaptateur femelle RJ-45 à DB-9.

Les paramètres par défaut du port console sont 9600 bauds, 8 bits de données, sans parité, 1 bit d'arrêt, et sans contrôle de flux. Le port console ne prend pas en charge le contrôle de flux matériel.

Procédez comme suit pour connecter un terminal au port console du routeur:

Étape 1 Connectez le terminal à l'aide du câble à paires inversées RJ-45 à RJ-45 et d'un adaptateur RJ-45 à DB-9 ou RJ-45 à DB-25. 1



Étape 2 Configurez le terminal ou le logiciel d'émulation de terminal PC à 9600 bauds, 8 bits de données, sans parité, 1 bit d'arrêt, et sans contrôle de flux.

Système d'exploitation	Logiciels
Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me	HyperTerminal (livré avec Windows), ProComm Plus
Windows 3.1	Terminal (livré avec Windows)
Macintosh	ProComm, VersaTerm, ZTerm (fourni séparément)
Unix/Linux	Minicom

La Figure 2 présente une liste des systèmes d'exploitation et du logiciel d'émulation de terminal qui peuvent être utilisés.

Activité de TP

Exercice : Établissement d'une session en mode console avec HyperTerminal

Au cours de ce TP, les étudiants vont connecter un routeur et une station de travail en utilisant un câble console. Ils configureront ensuite HyperTerminal afin d'établir une session en mode console avec le routeur.

2.2 Démarrage d'un routeur

2.2.5 Connexion au routeur

Pour configurer les routeurs Cisco, vous devez accéder à leur interface utilisateur à l'aide d'un terminal ou via un accès à distance. Lors de l'accès, l'utilisateur doit se connecter au routeur avant de pouvoir entrer d'autres commandes.

Pour des raisons de sécurité, le routeur offre deux niveaux d'accès aux commandes :

- **Mode utilisateur:** Les tâches types comprennent notamment la vérification du fonctionnement du routeur. Ce mode ne permet pas de modifier la configuration du routeur.

- **Mode privilégié:** Les tâches types comprennent notamment la modification de la configuration du routeur.

L'invite du mode utilisateur s'affiche lors de la connexion au routeur. [1] Les commandes disponibles à ce niveau sont un sous-ensemble des commandes disponibles en mode privilégié. La plupart de ces commandes vous permettent d'afficher des données sans changer les paramètres de configuration du routeur.

Pour pouvoir accéder à l'ensemble des commandes, vous devez activer le mode privilégié. À l'invite >, tapez **enable**. À l'invite **password:** , entrez le mot de passe qui a été défini à l'aide de la commande **enable secret**. Deux commandes permettent de définir un mot de passe d'accès au mode privilégié: **enable password** et **enable secret**. Si les deux commandes sont utilisées, la commande enable secret a préséance. Une fois les étapes de connexion terminées, l'invite devient #, ce qui indique que le mode privilégié est actif. Il n'est possible d'accéder au mode de configuration globale qu'à partir du mode privilégié. Il est possible, à partir du mode de configuration globale, d'accéder aux modes spécifiques suivants:

- Interface
- Sous-interface
- Ligne
- Routeur
- Mise en correspondance de route

Pour retourner au mode utilisateur à partir du mode privilégié, vous devez entrer la commande **disable**. Pour retourner au mode privilégié à partir du mode de configuration globale, tapez **exit** ou **Ctrl-Z**. Cette combinaison de touches peut également être utilisée pour retourner directement au mode privilégié à partir de n'importe quel sous-mode de configuration globale.

2.2 Démarrage d'un routeur

2.2.6 Aide au clavier dans l'interface de commande en ligne du routeur

Si vous entrez un point d'interrogation (?) à l'invite du mode utilisateur ou du mode privilégié, la liste des commandes disponibles s'affiche à l'écran. [1] Remarquez la ligne **--More--** au bas de l'exemple. L'écran affiche plusieurs lignes à la fois. L'invite **--More--** en bas de l'affichage indique la présence de plusieurs écrans. Chaque fois qu'une invite **--More--** apparaît, l'écran suivant peut être affiché en appuyant sur la barre d'espacement. Pour afficher uniquement la ligne suivante, appuyez sur la touche **Entrée**. Appuyez sur une autre touche pour retourner à l'invite. [1]

Routeur

```
Cisco>?
Exec commands:
access-enable     Create a temporary Access-List
                  entry
access-profile    Apply user-profile to interface
access-template   Create a temporary Access-List
                  entry
archive           manage archive files
bfe               For manual emergency modes
                  setting
cd                Change current directory
clear             Reset functions
clock             Manage the system clock
configure         Enter configuration mode
connect           Open a terminal connection
copy              Copy from one file to another
--More--
debug             Debugging functions (see also
                  'undebug')
delete            Delete a file
dir               List files on a filesystem
disable           Turn off privileged commands
disconnect        Disconnect an existing network
                  connection
elog              Event-logging control commands
enable            Turn on privileged commands
erase             Erase a filesystem
exit              Exit from the EXEC
help              Description of the interactive
                  help system
isdn              Make/disconnect an ISDN data call
                  on a BRI interface
lock              Lock the terminal
login             Log in as a particular user
logout            Exit from the EXEC
more              Display the contents of a file
mrinfo            Request neighbor and version
                  information from a multicast
                  router
mrm               IP Multicast Routing Monitor Test
mstat             Show statistics after multiple
                  multicast traceroutes
mtrace            Trace reverse multicast path from
                  destination to source
name-connection   Name an existing network
                  connection
no                Disable debugging functions
pad               Open a X.29 PAD connection
ping              Send echo messages
ppp               Start IETF Point-to-Point
                  Protocol (PPP)
```

```
pwd             Display current working directory
reload          Halt and perform a cold restart
resume          Resume an active network
                connection
rlogin          Open an rlogin connection
rsh             Execute a remote command
send            Send a message to other tty lines
setup           Run the SETUP command facility
show            Show running system information
slip            Start Serial-line IP (SLIP)
start-chat      Start a chat-script on a line
systat          Display information about
                terminal lines
telnet          Open a telnet connection
terminal        Set terminal line parameters
test            Test subsystems, memory, and
                interfaces
traceroute      Trace route to destination
tunnel          Open a tunnel connection
udptn           Open an udptn connection
undebug         Disable debugging functions (see
                also 'debug')
verify          Verify a file
where           List active connections
write           Write running configuration to
                memory, network, or terminal
x28             Become an X.28 PAD
x3              Set X.3 parameters on PAD
```

Pour accéder au mode privilégié, tapez **enable** ou l'abréviation **ena**. Le routeur demandera alors un mot de passe à l'utilisateur (si ce mot de passe a été défini). Si un **?** (point d'interrogation) est tapé à l'invite du mode privilégié, la liste des commandes affichée est plus longue que celle qui s'afficherait en mode utilisateur.

Routeur

```
Cisco#?
Exec commands:
  access-enable    Create a temporary Access-List
                   entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List
                   entry
  archive          manage archive files
  bfe              For manual emergency modes
                   setting
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  debug            Debugging functions (see also
                   'undebug')
  delete           Delete a file
  dir              List files on a filesystem
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network
                   connection
  elog             Event-logging control commands
  enable           Turn on privileged commands
  erase            Erase a filesystem
  exit             Exit from the EXEC
  help             Description of the interactive
                   help system
 --More--
```

Les données affichées varient selon la version de la plate-forme logicielle Cisco IOS et la configuration du routeur.

Si un utilisateur veut régler l'horloge du routeur mais qu'il ne sait pas quelle commande utiliser pour cela, il peut utiliser la fonction d'aide. 3L'exercice qui suit illustre l'une des nombreuses utilisations de la fonction d'aide.

Routeur

```
Cisco#cl?
clear  clock
Cisco#clock
% Incomplete command.
Cisco#clock ?
  set  Set the time and date
Cisco#clock set
% Incomplete command.
Cisco#clock set ?
  hh:mm:ss  Current Time
```

Vous devez régler l'horloge du routeur En supposant que vous ne connaissez pas la commande, procédez comme suit :

Étape 1 Utilisez **?** pour trouver la commande de réglage de l'horloge. Le texte d'aide indique qu'il faut utiliser la commande **`clock`**.

Étape 2 Vérifiez la syntaxe relative au réglage de l'heure.

Étape 3 Entrez l'heure en précisant l'heure, les minutes et les secondes, comme l'illustre la figure 4. Le système indique que des informations supplémentaires doivent être fournies pour utiliser la commande.

Routeur

```
Cisco#clock set 19:50:00
% Incomplete command.
Cisco#clock set 19:50:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year
Cisco#clock set 19:50:00 14 7
                            ^
% Invalid input detected at '^' marker.
Cisco#clock set 19:50:00 14 July
% Incomplete command.
Cisco#clock set 19:50:00 14 July ?
  <1993-2035>  Year
Cisco#clock set 19:50:00 14 July 2003
Cisco#
```

Étape 4 Appuyez sur **Ctrl-P** (ou la flèche vers le haut) pour répéter automatiquement la commande précédente. Entrez ensuite un espace et un point d'interrogation (?) pour afficher les arguments supplémentaires. L'entrée de la commande peut alors être terminée.

Étape 5 L'accent circonflexe (^) et la réponse fournie par l'aide en ligne indiquent une erreur. La position de l'accent circonflexe indique l'emplacement du problème éventuel. Pour trouver la syntaxe correcte, entrez de nouveau la commande jusqu'au niveau de l'accent circonflexe et entrez un point d'interrogation (?).

Étape 6 Entrez l'année, en respectant la syntaxe appropriée, puis appuyez sur **Entrée** afin d'exécuter la commande.

Activité de TP

Activité en ligne : Aide au clavier dans l'interface de commande en ligne

L'objectif de ce TP est de se familiariser avec le système d'aide de l'IOS.

Activité de TP

Activité en ligne : Fonction d'auto-complétion de l'IOS

Au cours de ce TP, vous allez apprendre à utiliser la fonction d'auto-complétion (touche de tabulation) et l'historique.

2.2 Démarrage d'un routeur

2.2.7 Commandes d'édition avancée

L'interface utilisateur offre un mode d'édition avancée vous permettant de modifier une ligne de commande au cours de la frappe. Utilisez les séquences de touches illustrées à la figure 1 pour placer le curseur sur la ligne de commande afin d'apporter des corrections ou des modifications. Le mode d'édition avancée est automatiquement activé dans la version actuelle du logiciel. Vous pouvez toutefois le désactiver en cas d'interférence avec vos scripts. Pour désactiver le mode d'édition avancée, entrez la commande **`terminal no editing`** à l'invite du mode privilégié.

Commande	Description
Ctrl-A	Permet de revenir au début de la ligne de commande.
Esc-B	Permet de reculer d'un mot.
Ctrl-B (ou flèche gauche)	Permet de reculer d'un caractère.
Ctrl-E	Permet d'atteindre la fin de la ligne de commande.
Ctrl-F (ou flèche droite)	Permet d'avancer d'un caractère.
Esc-F	Permet d'avancer d'un mot.

Le mode d'édition offre une fonction de défilement horizontal pour les commandes qui occupent plus d'une ligne à l'écran. Lorsque le curseur atteint la marge de droite, la ligne de commande se déplace vers la gauche de dix espaces. Les 10 premiers caractères de la ligne sont alors cachés, mais il est possible de faire défiler la ligne en sens inverse pour vérifier la syntaxe du début de la commande. Pour défiler en sens inverse, appuyez plusieurs fois sur **Ctrl-B** ou sur la flèche vers la gauche pour vous déplacer jusqu'au début de la commande. Vous pouvez également appuyer sur **Ctrl-A** pour retourner directement en début de ligne.

Routeur

```
Router>$ value for our customers and employees
```

Dans l'exemple de la figure 2, la commande occupe plus d'une ligne. Lorsque le curseur atteint la marge de droite, la ligne se déplace vers la gauche de dix espaces avant d'être affichée de nouveau. Le symbole du dollar (**$**) indique que la ligne a été déplacée vers la gauche. Chaque fois que le curseur atteint la marge de droite, la ligne se déplace de nouveau vers la gauche de dix espaces.

Les données affichées varient selon la version de la plate-forme logicielle Cisco IOS et la configuration du routeur.

Ctrl-Z est une commande utilisée pour quitter le mode de configuration. Elle permet de retourner au mode privilégié.

Activité de média interactive

Glisser-Positionner : Commandes d'édition avancées

À la fin de cette activité, l'étudiant doit être en mesure d'identifier l'usage approprié des commandes d'édition avancée.

2.2 Démarrage d'un routeur

2.2.8 Historique des commandes du routeur

L'interface utilisateur fournit l'historique des commandes qui ont été saisies. Cette fonction s'avère particulièrement utile pour rappeler des commandes ou des entrées longues ou complexes. La fonction d'historique des commandes vous permet d'accomplir les tâches suivantes:

- définir la capacité du tampon d'historique des commandes,
- rappeler des commandes,
- désactiver la fonction d'historique des commandes.

Par défaut, la fonction d'historique des commandes est active et le système enregistre 10 lignes de commandes dans son tampon. Pour changer le nombre de lignes de commandes enregistrées par le système au cours d'une session de terminal, utilisez la commande **`terminal history size`** ou **`history size`**. 1 Le nombre maximum de commandes est de 256.

Commande	Description
Ctrl-P ou flèche vers le haut	Rappelle la dernière commande (commande précédente).
Ctrl-N ou flèche vers le bas	Rappelle la dernière commande la plus récente.
Router>**show history**	Affiche la mémoire tampon des commandes.
Router>**terminal history size** *number-of-lines*	Définit la taille de la mémoire tampon historique des commandes*
Router>**terminal no editing**	Désactive les fonctions d'édition avancées.
Router>**terminal editing**	Re-enables advanced editing
<Tab>	Complète l'entrée.

*Le nombre varie en fonction de ce qui est affiché sur l'écran de l'utilisateur

Pour rappeler des commandes du tampon d'historique, en commençant par la dernière saisie, appuyez sur **Ctrl-P** ou sur la flèche vers le haut. Appuyez plusieurs fois sur ces touches afin de rappeler des commandes plus anciennes. Pour retourner aux commandes plus récentes du tampon, après le rappel de commandes au moyen de **Ctrl-P** ou de la flèche vers le haut, appuyez plusieurs fois sur **Ctrl-N** ou sur la flèche vers le bas. Cela a pour effet d'afficher des commandes de plus en plus récentes.

Pour gagner du temps lorsque vous tapez des commandes, vous pouvez entrer les caractères uniques de la commande. Appuyez sur touche **Tab**, et l'interface complètera l'entrée pour vous. Lorsque les lettres tapées identifient la commande de façon unique, la touche de tabulation ne fait que confirmer visuellement que le routeur a compris de quelle commande il s'agissait.

La plupart des ordinateurs offrent des fonctions supplémentaires de copie et de sélection. Vous pouvez copier une chaîne de commandes saisie précédemment et la coller ou l'insérer comme commande à exécuter.

Activité de média interactive

Glisser-Positionner : Historique des commandes du routeur

À la fin de cette activité, l'étudiant doit être en mesure d'identifier l'utilisation correcte des frappes de touches liées à l'historique des commandes.

2.2 Démarrage d'un routeur

2.2.9 Résolution des erreurs sur la ligne de commande

Les erreurs sur la ligne de commande ont pour principale origine les erreurs de frappe. Si le mot clé d'une commande est tapé incorrectement, l'interface utilisateur isole l'erreur à l'aide d'un indicateur (^). Ce signe est inséré dans la chaîne de commande, à l'endroit où se trouve une commande, un mot clé ou un argument erroné. L'indicateur d'erreur et le système d'aide en ligne vous permettent de localiser et de corriger aisément les erreurs de syntaxe.

```
Router#clock set 13:32:00 23 February 99
                                       ^
```

% Invalid input detected at "^" marker.

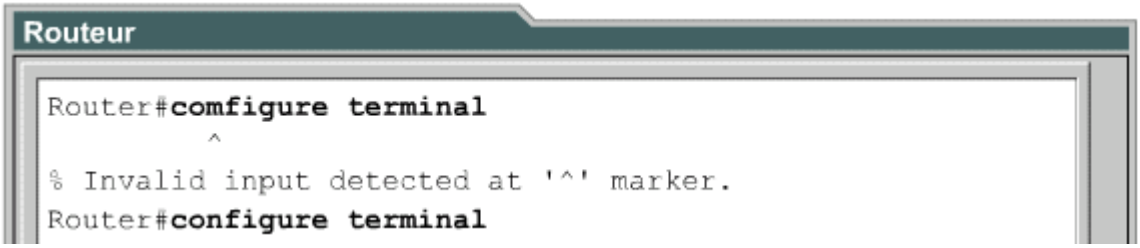
L'accent circonflexe (^) et la réponse fournie par l'aide en ligne indiquent une erreur à la ligne 93. Pour trouver la syntaxe correcte, entrez de nouveau la commande jusqu'au niveau de l'accent circonflexe et entrez un point d'interrogation (?) :

```
Router#clock set 13:32:00 23 February ?
<1993-2035> Year
Router#clock set 13:32:00 23 February
```

Entrez l'année, en utilisant la syntaxe appropriée, puis appuyez sur **Entrée** afin d'exécuter la commande.

```
Router#clock set 13:32:00 23 February 1999
```

Si une ligne de commande est entrée de façon incorrecte et que vous appuyez sur la touche **Entrée**, vous pouvez appuyer sur la touche vers le haut pour répéter la dernière commande. Utilisez les touches vers la droite ou vers la gauche pour déplacer le curseur vers l'emplacement où l'erreur a été faite. Tapez ensuite la correction nécessaire. Si une suppression est nécessaire, utilisez la touche <Retour arrière>.



Activité de TP

Exercice : Principes fondamentaux de la ligne de commande

Au cours de ce TP, l'étudiant va se connecter à un routeur en mode utilisateur et en mode privilégié, puis utiliser diverses commandes de routeur de base pour déterminer comment le routeur est configuré.

2.2 Démarrage d'un routeur

2.2.10 La commande show version

La commande **show version** affiche les informations relatives à la version de l'IOS actuellement chargée dans le routeur. Il s'agit notamment du registre de configuration et de la valeur du champ de démarrage.

La figure 1 présente les informations suivantes à propos de la commande **show version**:

- la version de l'IOS et informations descriptives,
- la version de ROM du bootstrap,
- la version de la ROM amorçable,
- le temps de fonctionnement du routeur,
- la dernière méthode de redémarrage,
- le fichier et l'emplacement de l'image système,
- la plate-forme de routeur,
- la valeur du registre de configuration.

Utilisez la commande **show version** pour identifier l'image IOS et la source de démarrage du routeur.

Routeur

```
GAD#show version
Cisco Internetwork Operating System Software
IOS (tm) 1700 Software (C1700-BNSY-L), Version
12.2(11)P, RELEASE SOFTWARE (fc1)
… <output omitted>…
ROM: System Bootstrap, Version 11.1(10)AA, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)
ROM: 1700 Software (C1700-BOOT-R), Version
11.1(10)AA, EARLY DEPLOYMENT RELEASE SOFTWARE
(fc1)
GAD uptime is 3 weeks 6 days 2 hours, 11 minutes
System restarted by power-on
System image file is "flash:c1700-bnsy-l.122-
11.p", booted via flash
cisco 1721 (68360) processor (revision C) with
3584K/512K bytes of memory.
Processor board ID 12014633, with hardware
revision 00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP
compliant.
1 Ethernet/IEEE 802.3 interface(s)
2  serial(sync/async) network interface(s)
System/IO memory with parity disabled
2048K bytes of DRAM onboard 2048K bytes of DRAM on
SIMM
System running from FLASH
8K bytes of non-volatile configuration memory.
6144K bytes of processor board PCMCIA flash (Read
ONLY)

Configuration register is 0x2102

GAD#
```

Résumé

La compréhension des points clés suivants devrait être acquise :

- Rôle de l'IOS
- Fonctionnement de base de l'IOS
- Identification des diverses fonctions de l'IOS
- Identification des méthodes permettant d'établir une session CLI avec le routeur
- Différences entre les modes utilisateur et privilégié
- Établissement d'une session HyperTerminal
- Connexion au routeur
- Utilisation de la fonction d'aide dans l'interface de commande en ligne
- Utilisation des commandes d'édition avancée
- Utilisation de l'historique des commandes
- Résolution des erreurs sur la ligne de commandes
- Utilisation de la commande **`show version`**

Résumé

- La plate-forme logicielle Cisco IOS contrôle les fonctions de routage et de commutation des unités d'une interconnexion de réseaux.
- La plate-forme logicielle Cisco IOS utilise une interface de ligne de commande comme environnement de console traditionnel.
- La plate-forme logicielle Cisco IOS a deux niveaux d'accès : le mode utilisateur et le mode privilégié.
- Pour démarrer, un routeur doit charger le programme bootstrap, le système d'exploitation et un fichier de configuration.
- Les routeurs Cisco utilisent des indicateurs LED pour fournir des informations d'état.

Vue d'ensemble

Il peut s'avérer assez difficile de configurer un routeur pour lui faire exécuter des tâches de réseau complexes. Toutefois, les premières procédures sont plutôt simples. Une bonne pratique des procédures et des étapes qui permettent de basculer entre les différents modes d'un routeur vous permettra d'aborder en confiance les configurations les plus complexes. Ce module présente les modes de configuration de base d'un routeur et offre l'occasion d'opérer des configurations simples.

Les administrateurs réseau doivent avoir comme objectif de réaliser une configuration de routeur claire et facile à comprendre, qui est sauvegardée de façon régulière. La plate-forme logicielle Cisco IOS fournit à l'administrateur plusieurs outils pour insérer des informations dans le fichier de configuration à des fins de documentation. À l'instar du développeur compétent qui documente chaque étape de sa programmation, l'administrateur doit fournir un maximum d'informations en prévision de l'éventuelle prise en main du réseau par une autre personne.

À la fin de ce module, les étudiants doivent être en mesure de :

- Nommer un routeur
- Définir des mots de passe
- Examiner les commandes show
- Configurer une interface série
- Configurer une interface Ethernet
- Apporter des modifications au routeur
- Enregistrer les modifications apportées à un routeur
- Configurer une description d'interface
- Configurer une bannière du message du jour
- Configurer des tables d'hôtes
- Comprendre l'importance des sauvegardes et de la documentation

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
3.1	Configuration d'un routeur
3.2	Finalisation de la configuration

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
	• Configuration d'adresses IP, de masques de sous-réseau et d'adresses de passerelles sur des routeurs et des hôtes • Configuration d'un routeur en vue de fonctionnalités d'administration supplémentaires • Mise en œuvre d'un LAN • Gestion des fichiers de configuration des équipements et de l'image système • Création d'une configuration initiale sur un routeur		

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception ou modification d'un LAN simple à l'aide de produits Cisco	• Configuration d'adresses IP, de masques de sous-réseau et d'adresses de passerelles sur des routeurs et des hôtes • Configuration d'un routeur en vue de fonctionnalités d'administration supplémentaires • Mise en œuvre d'un LAN		

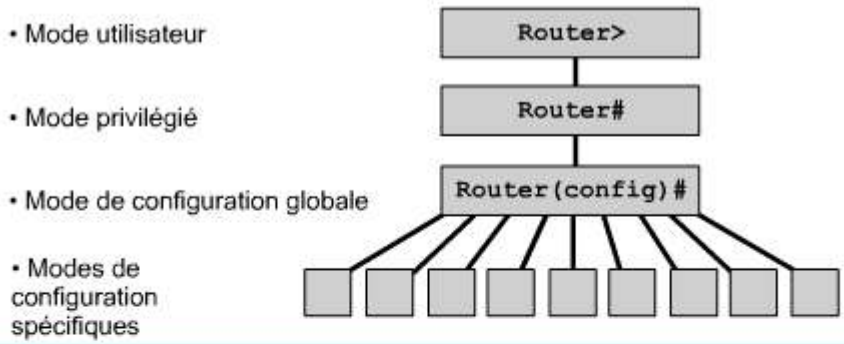
Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
	• Établissement de communication entre un équipement terminal et l'IOS du routeur, et utilisation de l'IOS en vue de l'analyse du système • Manipulation des fichiers de configuration des équipements et de l'image système • Création d'une configuration initiale sur un routeur et enregistrement du fichier de configuration obtenu	

3.1 Configuration d'un routeur

3.1.1 modes de commande CLI

Toutes les modifications de la configuration de l'interface de commande en ligne (CLI) apportées sur un routeur Cisco sont effectuées en mode de configuration globale. D'autres modes spécifiques sont activés en fonction de la modification de configuration requise, mais ces modes sont tous des sous-ensembles du mode de configuration globale. 1



Mode de configuration	Invite
Interface	Router(config-if)#
Sous-interface	Router(config-subif)#
Contrôleur	Router(config-controller)#
Liste de mise en correspondance	Router(config-map-list)#
Classe de mise en correspondance	Router(config-map-class)#
Ligne	Router(config-line)#
Routeur	Router(config-router)#
Routeur IPX	Router(config-ipx-router)#
Mise en correspondance de route	Router(config-route-map)#

Les commandes de configuration globale sont utilisées sur un routeur pour appliquer des instructions de configuration qui affectent l'ensemble du système. La commande suivante place le routeur en mode de configuration globale et permet d'entrer des commandes à partir du terminal :

REMARQUE:
L'invite change pour indiquer que le routeur est à présent en mode de configuration globale.

```
Router#configure terminal
Router(config)#
```

Le mode de configuration globale (global config) est le mode de configuration principal. Voici quelques-uns des modes auquel vous pouvez accéder à partir du mode de configuration globale:

- Mode interface
- Mode ligne
- Mode routeur
- Mode sous-interface
- Mode contrôleur

Lorsque vous passez dans ces modes spécifiques, l'invite du routeur se transforme pour indiquer le mode de configuration particulier. Toute modification de la configuration effectuée s'applique uniquement aux interfaces ou aux processus couverts par le mode particulier.

Si vous tapez **exit** alors que vous êtes dans l'un de ces modes de configuration spécifiques, le routeur retourne en mode de configuration globale. Si vous appuyez sur les touches **Ctrl-Z**, vous quittez les modes de configuration et vous revenez au mode privilégié.

3.1 Configuration d'un routeur

3.1.2 Configuration du nom d'un routeur

L'une des premières tâches de configuration consiste à attribuer au routeur un nom unique. Pour ce faire, vous devez, en mode de configuration globale, utiliser les commandes suivantes:


```
Router(config)#hostname Tokyo
Tokyo(config)#
```

Dès que vous appuyez sur la touche **Entrée**, l'invite passe du nom d'hôte par défaut (Router) au nom d'hôte nouvellement configuré, c'est-à-dire Tokyo, dans notre exemple.

Activité de TP

Exercice : Modes de commande et identification d'un routeur

L'objectif de ce TP est d'identifier les modes de base des routeurs que sont le mode utilisateur et le mode privilégié, puis d'utiliser des commandes pour activer des modes spécifiques.

3.1 Configuration d'un routeur

3.1.3 Configuration des mots de passe d'un routeur

Les mots de passe limitent l'accès aux routeurs. Ils doivent toujours être configurés pour les lignes de terminal virtuel et pour la ligne de console. Les mots de passe sont également utilisés pour contrôler l'accès au mode privilégié pour que seuls les utilisateurs autorisés puissent apporter des modifications au fichier de configuration.

Les commandes suivantes permettent de définir un mot de passe facultatif mais recommandé sur la ligne de console :

```
Router(config)#line console 0
Router(config-line)#password <password>
Router(config-line)#login
```

Pour que les utilisateurs puissent accéder à distance au routeur à l'aide de Telnet, un mot de passe doit être défini sur une ou plusieurs lignes de terminal virtuel (VTY). En règle générale, les routeurs Cisco prennent en charge cinq lignes VTY numérotées de 0 à 4, bien que chaque plate-forme matérielle prenne en charge des numéros différents sur les connexions VTY. Le même mot de passe est souvent utilisé pour toutes les lignes, mais il arrive parfois qu'une ligne soit définie pour fournir au routeur une entrée de secours si les quatre autres connexions sont utilisées. Les commandes suivantes sont utilisées pour définir le mot de passe sur les lignes VTY:

```
Router(config)#line vty 0 4
Router(config-line)#password <password>
Router(config-line)#login
```

Le mot de passe enable et le mot de passe enable secret sont utilisés pour limiter l'accès au mode privilégié. Seul le mot de passe enable est utilisé si le mot de passe enable secret n'a pas été défini. Il est recommandé de définir et d'utiliser uniquement le mot de passe enable secret car, contrairement au mot de passe enable, il est crypté. Les commandes suivantes permettent de définir les mots de passe enable :

```
Router(config)#enable password <password>
Router(config)#enable secret <password>
```

Il est parfois préférable que les mots de passe ne soient pas affichés en texte clair dans le résultat des commandes **show running-config** ou **show startup-config**. Cette commande permet de crypter les mots de passe dans le résultat de configuration:

```
Router(config)#service password-encryption
```

La commande **service password-encryption** applique un cryptage simple à tous les mots de passe non cryptés. La commande **enable secret**<*password*> utilise un puissant algorithme MD5 pour le cryptage.

Mot de passe de console

```
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
```

Mot de passe de terminal virtuel

```
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
```

Mot de passe enable

```
Router(config)#enable password san-fran
```

Cryptage d'un mot de passe

```
Router(config)#service password-encryption
Router(config)#enable secret <password>
```

Activité de TP

Exercice : Configuration des mots de passe d'un routeur

L'objectif de ce TP est de configurer un mot de passe pour la connexion de console en mode utilisateur, puis un mot de passe pour des sessions de terminal virtuel (Telnet).

3.1 Configuration d'un routeur

3.1.4 Examen des commandes show

Plusieurs commandes **show** peuvent être utilisées pour examiner le contenu des fichiers du routeur ou pour le dépannage. Dans le mode privilégié et le mode utilisateur, la commande **show ?** présente une liste des commandes **show** disponibles. Cette liste est beaucoup plus longue en mode privilégié qu'en mode utilisateur.

- **show interfaces**: Affiche les statistiques relatives à toutes les interfaces du routeur. Pour afficher les statistiques d'une interface spécifique, entrez la commande **show interfaces**, suivie par le numéro spécifique de l'interface et du port. Exemple:

```
Router#show interfaces serial 0/1
```

- **show controllers serial**:Affiche les caractéristiques de l'interface. Cette commande doit indiquer le port ou l'emplacement et le numéro de port (slot/port number) de l'interface série. Par exemple:

  ```
  Router#show controllers serial 0/1
  ```

- **show clock**: Indique l'heure définie sur le routeur
- **show hosts**: Affiche une liste de noms et d'adresses d'hôtes se trouvant en mémoire cache
- **show users**: Indique tous les utilisateurs connectés au routeur
- **show history**: Affiche un historique des commandes qui ont été saisies
- **show flash**: Affiche des informations sur la mémoire flash ainsi que la liste des fichiers IOS qui y sont stockés
- **show version**: Affiche des informations sur le logiciel actuellement chargé en mémoire ainsi que sur les caractéristiques du matériel et de l'équipement.
- **show ARP**: Affiche la table ARP du routeur
- **show protocols**: Affiche l'état général et propre aux interfaces de tous les protocoles de couche 3 configurés.
- **show startup-config**: Affiche le contenu de la NVRAM si elle est disponible et valide ou montre le fichier de configuration référencé par la variable d'environnement CONFIG_FILE.
- **show running-config**: Affiche le contenu du fichier de configuration exécuté actuellement en mémoire.

Router

```
LAB_A#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(9),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Mon 24-Jan-00 22:06 by bettyl
Image text-base: 0x030387D0, data-base: 0x00001000

ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), Version
10.2(8a), RELEASE SOFTWARE (fc1)

LAB_A uptime is 25 minutes
System restarted by reload
System image file is "flash:c2500-d-l_120-9.bin"

cisco 2500 (68030) processor (revision D) with
8192K/2048K bytes of memory.
Processor board ID 02001682, with hardware revision
00000000
Bridging software.
X.25 software, Version 3.0.0.
2 Ethernet/IEEE 802.3 interface(s)
2 Serial network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read ONLY)
Configuration register is 0x2102
LAB_A#show flash
System flash directory:
File  Length   Name/status
  1   6888660  c2500-d-l_120-9.bin
[6888724 bytes used, 1499884 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
LAB_A#show users
    Line      User       Host(s)              Idle Location
*   0 con 0               idle                  00:00:00

LAB_A#
```

Activité de TP

Exercice : Utilisation des commandes de routeur show

L'objectif de ce TP est de vous faire connaître les commandes de base de routeur show.

Activité de TP

Activité en ligne : Paramètres par défaut

L'objectif de ce TP est d'afficher les détails de configuration et d'interface de base pour visualiser les valeurs par

défaut du routeur.

3.1 Configuration d'un routeur

3.1.5 Configuration d'une interface série

Une interface série peut être configurée depuis la console ou par l'intermédiaire d'une ligne de terminal virtuel. Pour configurer une interface série, procédez comme suit:

1. Passez en mode de configuration globale
2. Passez en mode interface
3. Spécifiez l'adresse et le masque de sous-réseau de l'interface
4. Si un câble ETCD est connecté, définissez la fréquence d'horloge. Ignorez cette étape si c'est un câble ETTD qui est connecté.
5. Activez l'interface

Dans les commandes suivantes, l'argument Type peut être remplacé par " serial, ethernet, fastethernet, token ring ", etc. :

```
Router(config)#interface type port
Router(config)#interface type slot/port
```

La commande suivante permet de désactiver l'interface au niveau administratif :

```
Router(config-if)#shutdown
```

La commande suivante permet d'activer une interface qui a été désactivée :

```
Router(config-if)#no shutdown
```

La commande suivante permet de quitter le mode de configuration d'interface actuel :

```
Router(config-if)#exit
```

Si l'interface est destinée à acheminer des paquets IP, chaque interface série connectée doit posséder une adresse IP et un masque de sous-réseau. Configurez l'adresse IP à l'aide des commandes suivantes :

```
Router(config)#interface serial 0/0
Router(config-if)#ip address <ip address> <net mask>
```

Les interfaces série nécessitent un signal d'horloge pour contrôler la synchronisation des communications. Dans la plupart des environnements, un équipement ETCD tel qu'une CSU fournira cette synchronisation. Par défaut, les routeurs Cisco sont des équipements ETTD, mais ils peuvent être configurés en tant qu'équipements ETCD.

Sur les liaisons série qui sont directement interconnectées, comme dans un environnement de TP, un des côtés doit être considéré comme un équipement ETCD et fournir le signal de synchronisation. L'horloge est activée et sa fréquence est spécifiée à l'aide de la commande **clock rate**. Les fréquences d'horloge (en bits par seconde) sont les suivantes : 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000 ou 4000000. Cependant, certains de ces paramètres peuvent ne pas être disponibles sur certaines interfaces série, en raison de leur capacité.

Par défaut, les interfaces sont mises hors tension ou désactivées. Pour mettre sous tension ou activer une interface, la commande **no shutdown** est exécutée. S'il est nécessaire de désactiver une interface en vue d'une opération de maintenance ou de dépannage, la commande **shutdown** est utilisée pour mettre l'interface hors tension.

Dans l'environnement de TP, nous utiliserons la valeur 56000 comme fréquence d'horloge. Les commandes qui permettent de définir une fréquence d'horloge et d'activer une interface série sont les suivantes:

```
Router(config)#interface serial 0/0
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
```

Activité de TP

Exercice : Configuration d'une interface série

Au cours de ce TP, l'étudiant va configurer une interface série sur les routeurs GAD et BHM pour leur permettre de communiquer.

Activité de TP

Activité en ligne : Configuration d'une interface série

L'objectif de ce TP est d'accéder à l'interface de commande en ligne du routeur et d'activer les options de configuration du niveau privilégié.

3.1 Configuration d'un routeur

3.1.6 Faire des changements de configuration

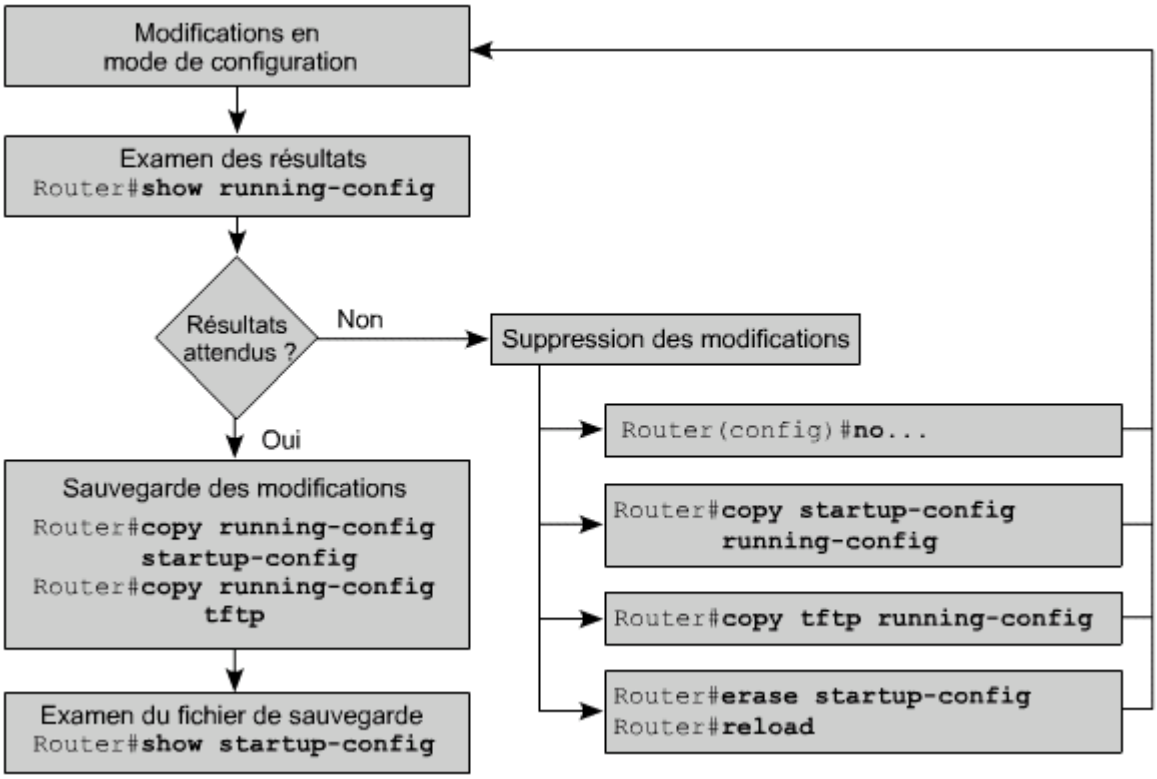
Si une configuration doit être modifiée, passez dans le mode approprié et exécutez la commande nécessaire. Par exemple, pour activer une interface, passez en mode de configuration globale, en mode interface, puis lancez la commande **no shutdown**.

Pour vérifier les modifications, utilisez la commande **show running-config**. Cette commande affiche la configuration courante. Si les variables affichées ne correspondent pas à celles prévues, vous pouvez corriger l'environnement en effectuant une ou plusieurs des opérations suivantes:

- entrer la forme négative (**no**) d'une commande de configuration,
- recharger le système afin de rétablir le fichier de configuration d'origine de la mémoire NVRAM,
- copier un fichier de configuration archivé à partir d'un serveur TFTP,
- supprimer le fichier de configuration de démarrage à l'aide de **erase startup-config**, puis le redémarrer et passer en mode setup.

Pour enregistrer les variables de configuration dans le fichier de configuration de démarrage de la mémoire NVRAM, entrez la commande suivante à l'invite du mode privilégié:

```
Router#copy running-config startup-config
```



Activité de TP

Exercice : Modifications de configuration

L'objectif de ce TP est de configurer certains paramètres de base sur un routeur et d'activer et de désactiver des interfaces

3.1 Configuration d'un routeur

3.1.7 Configuration d'une interface Ethernet

Une interface Ethernet peut être configurée depuis la console ou par l'intermédiaire d'une ligne de terminal virtuel.

Si l'interface est destinée à acheminer des paquets IP, chaque interface Ethernet doit posséder une adresse IP et un masque de sous-réseau.

Router

```
Router(config)#interface e0
Router(config-if)#ip address 183.8.126.2 255.255.255.128
Router(config-if)#no shutdown
```

Pour configurer une interface Ethernet, procédez comme suit:

1. Passez en mode de configuration globale
2. Passez en mode de configuration d'interface
3. Spécifiez l'adresse et le masque de sous-réseau de l'interface
4. Activez l'interface

Par défaut, les interfaces sont mises hors tension ou désactivées. Pour mettre sous tension ou activer une interface, la commande **`no shutdown`** est exécutée. S'il est nécessaire de désactiver une interface en vue d'une opération de maintenance ou de dépannage, la commande **`shutdown`** est utilisée pour mettre l'interface hors tension.

Activité de TP

Exercice : Configuration d'une interface Ethernet

L'objectif de ce TP est de configurer une interface Ethernet sur le routeur avec une adresse IP et un masque de sous-réseau.

Activité de TP

Activité en ligne : Configuration d'une interface Ethernet

Au cours de ce TP, les étudiants vont configurer une interface Ethernet sur un routeur.

3.2 Fin de la configuration

3.2.1 Importance des normes de configuration

Il est important, au sein d'une organisation, de mettre en place des normes relatives aux fichiers de configuration. Cela permet de contrôler le nombre de fichiers de configuration à gérer, le mode de stockage des fichiers et leur emplacement de stockage. 1

Une norme est un ensemble de règles ou de procédures largement répandues ou officialisées. Une organisation qui n'applique pas de normes s'expose au chaos en cas d'interruption de service.

Pour gérer un réseau, une norme de support centralisée est indispensable. La configuration, la sécurité, les performances et diverses autres questions doivent être gérées de façon adéquate pour que le réseau fonctionne sans heurt. La création de normes de cohérence permet de réduire la complexité des réseaux, les temps d'arrêt non planifiés et l'exposition à des événements qui peuvent avoir un impact négatif sur les performances.

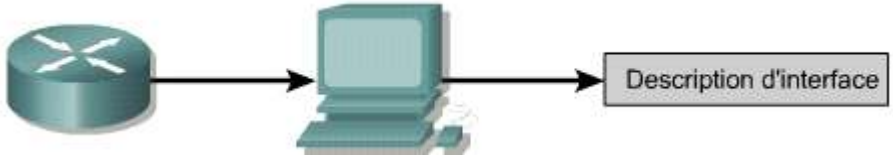
- Une norme est un ensemble de règles ou de procédures largement répandues ou officialisées.
- Une norme de configuration permet de structurer la topologie et de garantir le fonctionnement du réseau.

3.2 Fin de la configuration

3.2.2 Descriptions d'interface

Il est indispensable d'utiliser une description d'interface afin d'identifier des informations importantes concernant par exemple un routeur, un numéro de circuit ou un segment de réseau spécifique. En se reportant à cette description, un utilisateur de réseau pourra se souvenir d'informations spécifiques sur l'interface, telle que le réseau qu'elle dessert. 1

La description se limite à un commentaire à propos de l'interface. Bien qu'elle figure dans les fichiers de configuration qui sont stockés dans la mémoire du routeur, la description n'affecte en rien son fonctionnement. Les descriptions sont créées en respectant un format standard qui s'applique à chaque interface. La description peut inclure l'emplacement et le rôle de l'interface, les autres unités ou emplacements connectés à l'interface et les identificateurs de circuit. Grâce aux descriptions, les personnels de support comprennent mieux l'incidence des problèmes liés à une interface et peuvent résoudre les problèmes plus rapidement.



```
Tokyo(config)#interface e 0

Tokyo(config-if)#description Engineering LAN, Bldg. 18
```

3.2 Fin de la configuration

3.2.3 Configuration d'une description d'interface

Pour configurer une description d'interface, passez en mode configuration globale. À partir de ce mode, passez en mode de configuration d'interface. Utilisez la commande **description**, suivie des informations. 1

Procédure :

```
LAB_A>enable
Password:
LAB_A#configure terminal
Enter configuration commands, one per line.  End with
CNTL-Z.
LAB_A(config)#interface ethernet 0
LAB_A(config-if)#description LAN Engineering, Bldg. 2
LAB_A(config-if)#exit
LAB_A(config)#exit
LAB_A#show running-config
00:18:36: %SYS-5-CONFIG_I: Configured from console by
console
Building configuration...
```

Procédure :

```
interface Ethernet0
 description LAN Engineering, Bldg. 2
 ip address 192.5.5.1 255.255.255.0
 no ip directed-broadcast!
```

Étapes de la procédure:

Passez en mode de configuration globale en entrant la commande **configure terminal**.

Passez en mode d'interface spécifique (par exemple interface Ethernet 0) **interface ethernet 0**.

Entrez la description de la commande, suivie des informations que vous voulez voir s'afficher. Par exemple, Réseau XYZ, Immeuble 18.

Revenez en mode privilégié à l'aide de la commande **ctrl-Z**.

Enregistrez en mémoire NVRAM les modifications de la configuration à l'aide de la commande **copy running-config startup-config**.

Voici deux exemples de descriptions d'interface:

```
interface Ethernet 0
description LAN Engineering, Bldg.2
```

```
interface serial 0
description ABC network 1, Circuit 1
```

Activité de TP

Exercice : Configuration de descriptions d'interface

Au cours de ce TP, l'étudiant va s'exercer à choisir une description d'interface et à utiliser le mode de configuration d'interface pour entrer ensuite cette description.

3.2 Fin de la configuration

3.2.4 Bannières de connexion

Comme son nom l'indique, une bannière de connexion s'affiche lors de la connexion, et permet de transmettre un message destiné à tous les utilisateurs du routeur (pour les avertir, par exemple, d'un arrêt imminent du système).

Ces bannières de connexion peuvent être lues par tout le monde. Par conséquent, vous devez faire très attention à la formule choisie pour le message de la bannière. Un message "Bienvenue" qui invite tout le monde à entrer n'est probablement pas approprié. 1

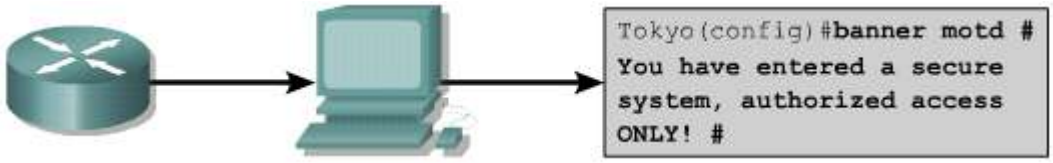
On préfèrera par exemple un avertissement indiquant de ne pas tenter de se connecter sans autorisation. Par exemple, un message tel que "Système sécurisé. Accès autorisé uniquement !" indique aux visiteurs indésirables que toute intrusion est interdite et illégale.

3.2 Fin de la configuration

3.2.5 Configuration du message du jour (MOTD)

Une bannière du message du jour (MOTD) peut être affichée sur tous les terminaux connectés.

Passez en mode de configuration globale pour configurer une bannière. Utilisez la commande **banner motd**, suivie d'un espace et d'un séparateur comme le signe dièse (#). Ajoutez un message du jour (MOTD), suivi d'un espace et du même séparateur. 1



Pour créer et afficher un message du jour, procédez comme suit:

1. Passez en mode de configuration globale en entrant la commande **configure terminal**.
2. Entrez la commande **banner motd # The message of the day goes here #**.
3. Enregistrez les modifications en lançant la commande **copy running-config startup-config**.

Activité de TP

Exercice : Configuration du message du jour (MOTD)

L'objectif de ce TP est d'entrer dans le routeur un message du jour (MOTD) qui sera vu par tous les utilisateurs lorsqu'ils se connecteront.

Activité de TP

Activité en ligne : Gestion interne

L'objectif de ce TP est d'implémenter des paramètres de configuration de base sur un routeur. Il s'agit notamment de définir les paramètres d'horloge du routeur, des descriptions d'interface et des messages du jour.

3.2 Fin de la configuration
3.2.6 Résolution de nom d'hôte

La résolution de nom d'hôte est le processus qu'utilise le système informatique pour associer un nom d'hôte à une adresse IP.

Pour pouvoir utiliser des noms d'hôtes afin de communiquer avec d'autres unités IP, les équipements réseau tels que les routeurs doivent être en mesure d'associer les noms d'hôte aux adresses IP. Une liste de noms d'hôtes et de leurs adresses IP associées a pour nom table d'hôtes. 1

Voici un exemple de configuration de table d'hôtes sur un routeur :

```
Router(config)#ip host Auckland 172.16.32.1
Router(config)#ip host Beirut 192.168.53.1
Router(config)#ip host Capetown 192.168.89.1
Router(config)#ip host Denver 10.202.8.1
```

Une table d'hôtes peut inclure tous les équipements d'une organisation de réseau. Un nom d'hôte peut être associé à chaque adresse IP unique. La plate-forme logicielle Cisco IOS conserve en mémoire cache les correspondances nom d'hôte-adresse de sorte que les commandes d'exécution puissent les utiliser. Cette mémoire cache accélère le processus de conversion des noms en adresses.

Contrairement aux noms DNS, les noms d'hôtes ne sont significatifs que sur le routeur sur lequel ils sont configurés. La table d'hôtes permettra à l'administrateur réseau de taper soit le nom d'hôte proprement dit, comme Auckland, soit l'adresse IP pour l'envoi d'une requête Telnet à un hôte distant. 1

3.2 Fin de la configuration
3.2.7 Configuration des tables d'hôtes

Pour attribuer des tables d'hôtes aux adresses, passez d'abord en mode de configuration globale. Entrez la commande **`ip host`**, suivie du nom de la destination et de toutes les adresses IP où l'équipement est accessible. Cela établit une correspondance entre le nom d'hôte et chacune de ses adresses IP d'interface. Pour atteindre l'hôte, utilisez la commande **`telnet`** ou **`ping`** avec le nom du routeur ou une adresse IP qui est associée au nom du routeur. 1

Router

```
LAB_A#show hosts
Default domain is not set
Name/address lookup uses domain service
Name servers are

Host      Flags        Age  Type  Address(es)
LAB_A     (perm, OK)   **   IP    192.5.5.1 205.7.5.1 201.100.11.1
LAB_B     (perm, OK)   **   IP    219.17.100.2 199.6.13.1 201.100.11.2
LAB_C     (perm, OK)   **   IP    223.8.151.1 204.204.7.1 199.6.13.2
LAB_D     (perm, OK)   **   IP    210.93.105.1 204.204.7.2
LAB_E     (perm, OK)   **   IP    210.93.105.2
```

Les adresses IP correspondent aux interfaces directement connectées sur chaque routeur de ce réseau.

La procédure de configuration de la table d'hôtes est la suivante: 2

Nom du routeur	Type de routeur	E0	E1	S0	S1
Lab_A	2514	192.5.5.1	205.7.5.1	201.100.11.1	--
Lab_B	2501	219.17.100.1	--	199.6.13.1	201.100.11.2
Lab_C	2501	223.8.151.1	--	204.204.7.1	199.6.13.2
Lab_D	2501	210.93.105.1	--	--	204.204.7.2
Lab_E	2501	210.93.105.2	--	--	--

1. Passez en mode de configuration globale sur le routeur.
2. Entrez la commande **`ip host`**, suivie du nom du routeur et de toutes les adresses IP associées aux interfaces sur chaque routeur.
3. Continuez jusqu'à ce que tous les routeurs du réseau soient entrés.
4. Enregistrez la configuration en mémoire NVRAM.

Activité de TP

Exercice : Configuration de tables d'hôtes

L'objectif de ce TP est de créer des tables d'hôtes IP associant des noms de routeurs à des adresses IP.

Activité de TP

Activité en ligne : Configuration de tables d'hôtes

Au cours de ce TP, l'étudiant va créer des tables d'hôtes IP qui permettent à un routeur d'utiliser des noms pour identifier toutes les interfaces qui lui sont connectées.

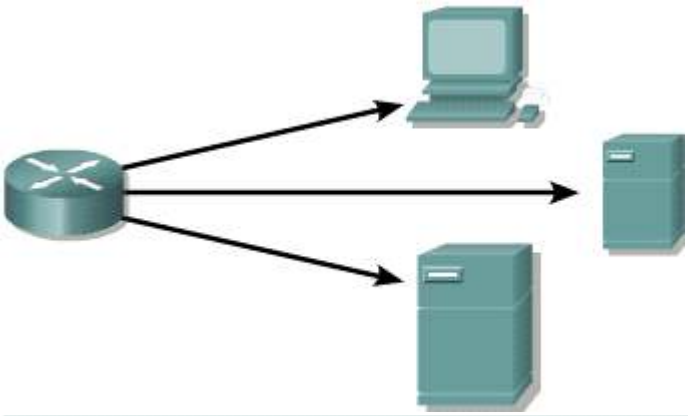
3.2 Fin de la configuration

3.2.8 Sauvegarde de la configuration et documentation

La configuration des équipements réseau détermine comment le réseau va se comporter. La gestion de la configuration des équipements comprend les tâches suivantes:

- Listage et comparaison les fichiers de configuration sur les équipements actifs
- Stockage des fichiers de configuration sur les serveurs de réseau
- Installations et mises à niveau de logiciels

Les fichiers de configuration doivent être stockés en tant que fichiers de sauvegarde pour parer à toute éventualité. Les fichiers de configuration peuvent être stockés sur un serveur réseau, sur un serveur TFTP ou encore sur un disque stocké en lieu sûr. 1La documentation doit être incluse avec ces informations hors connexion.



Enregistrez les fichiers de configuration sur :

- Un serveur TFTP
- Un serveur de réseau
- Un disque conservé dans un endroit sûr

3.2 Fin de la configuration

3.2.9 Copie, édition et collage des configurations

Une copie actuelle de la configuration peut être stockée sur un serveur TFTP. La commande **`copy running-config tftp`**, comme l'illustre la figure 1, peut être utilisée pour stocker la configuration actuelle sur le serveur TFTP du réseau. Pour ce faire, procédez comme suit :

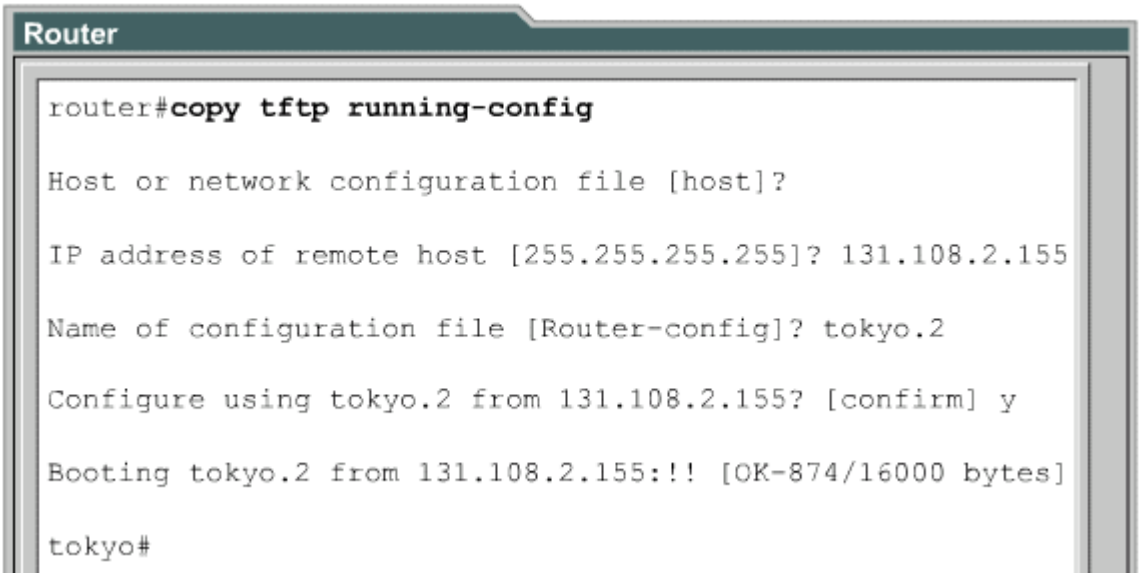
Router

```
Router#copy running-config tftp

Remote host []? 131.108.2.155

Name of configuration file to write[tokyo-config]?tokyo.2

Write file tokyo.2 to 131.108.2.155? [confirm] y

Writing tokyo.2 !!!!!! [OK]
```

Étape 1: Entrez la commande **`copy running-config tftp`**.
Étape 2: Entrez l'adresse IP de l'hôte où sera stocké le fichier de configuration.
Étape 3: Entrez le nom que vous voulez attribuer au fichier de configuration.
Étape 4: Confirmez vos choix en répondant oui à chaque fois.

Un fichier de configuration stocké sur l'un des serveurs du réseau peut être utilisé pour configurer un routeur. Pour ce faire, procédez comme suit:

1. Passez en mode configuration en entrant la commande **copy tftp running-config**, comme l'illustre la figure 2.



2. À l'invite du système, sélectionnez un fichier de configuration d'hôte ou de réseau. Le fichier de configuration de réseau comprend des commandes qui s'appliquent à tous les routeurs et serveurs de terminaux du réseau. Le fichier de configuration d'hôte comprend des commandes qui s'appliquent à un seul routeur. À l'invite du système, entrez l'adresse IP de l'hôte distant où se trouve le serveur TFTP. Dans cet exemple, le routeur est configuré à partir du serveur TFTP qui se trouve à l'adresse IP 131.108.2.155.
3. À l'invite du système, entrez le nom du fichier de configuration ou acceptez le nom par défaut. Le nom du fichier est basé sur les conventions d'appellation d'UNIX. Le nom de fichier par défaut est **hostname-config** pour le fichier hôte et **network-config** pour le fichier de configuration de réseau. Dans un environnement DOS, les noms de fichier sont limités à huit caractères, avec une extension de trois caractères (par exemple, **router.cfg**). Confirmez le nom du fichier de configuration et l'adresse du serveur TFTP fournis par le système. Dans la figure 2, notez que l'invite du routeur affiche immédiatement le nom **tokyo**. Vous avez ainsi la preuve que la reconfiguration est effective dès que le nouveau fichier est téléchargé.

La configuration du routeur peut être également sauvegardée en capturant le texte dans le routeur et en l'enregistrant sur une disquette ou sur un disque dur. Si vous devez recopier le fichier sur le routeur, utilisez les fonctions d'édition standard du programme émulateur de terminal pour coller le fichier de commandes dans le routeur.

Activité de TP

Exercice : Copie, édition et collage de configurations

L'objectif de ce TP est de capturer la configuration courante d'un routeur et de l'enregistrer dans un fichier texte ASCII à l'aide du programme HyperTerminal.

Résumé

Cette section résume les points clés de la configuration d'un routeur.

Le routeur comporte plusieurs modes d'exécution:

- Mode utilisateur
- Mode privilégié
- Mode de configuration globale
- Divers autres modes de configuration.

L'interface de commande en ligne peut être utilisée pour modifier la configuration:

- Définition du nom d'hôte
- Définition de mots de passe
- Configuration des interfaces
- Modication des configurations
- Affichage des configurations

La compréhension des points clés suivants devrait être acquise:

- Les normes de configuration sont des éléments clés du succès de toute organisation qui souhaite disposer d'un réseau efficace.
- Les descriptions d'interface peuvent comporter des informations importantes pour aider les administrateurs réseau à comprendre et dépanner leurs réseaux.
- Les bannières de connexion et les messages du jour fournissent des informations aux utilisateurs lorsqu'ils se connectent au routeur.
- Les résolutions de nom d'hôte traduisent les noms en adresses IP pour permettre au routeur de convertir rapidement les noms les noms en adresses.
- La sauvegarde et la documentation de la configuration sont cruciales pour un fonctionnement sans heurt du réseau.

Vue d'ensemble

Les administrateurs réseau se plaignent parfois du manque de précision et d'exhaustivité de la documentation de certains réseaux. Le protocole CDP (Cisco Discovery Protocol) peut s'avérer utile dans ses situations, en vous aidant à établir une représentation de base du réseau. CDP est un protocole propriétaire indépendant du média qui est utilisé pour la découverte du voisinage réseau. Il affiche uniquement des informations sur les équipements voisins directement connectés mais s'avère toutefois un outil puissant.

Dans de nombreux cas, après la configuration initiale d'un routeur, l'administrateur a du mal à s'y connecter directement pour apporter des modifications de configuration ou accomplir d'autres opérations. Telnet est une application TCP/IP qui permet de se connecter à distance à l'interface de commande en ligne (CLI) d'un routeur à des fins de configuration, de surveillance et de dépannage. Cet outil est indispensable pour le professionnel du réseau.

À la fin de ce module, les étudiants doivent être en mesure de:

- Activer et désactiver le protocole CDP
- Utiliser la commande **`show cdp neighbors`**
- Déterminer quels équipements voisins sont connectés à quelles interfaces locales
- Rassembler des informations d'adresse réseau sur les équipements voisins à l'aide du protocole CDP
- Établir une connexion Telnet
- Vérifier une connexion Telnet
- Se déconnecter d'une session Telnet
- Interrompre une session Telnet
- Exécuter des tests de connectivité alternative
- Dépanner les connexions de terminal à distance

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
4.1	Découverte du voisinage réseau et connexion
4.2	Obtention d'informations sur les équipements distants

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
		• Exécution du dépannage d'un LAN simple • Dépannage de l'adressage IP et de la configuration des hôtes • Dépannage d'un équipement dans un réseau en fonctionnement	

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
		• Exécution du dépannage d'un LAN et d'un VLAN • Dépannage de l'adressage IP et de la configuration des hôtes • Dépannage d'un équipement dans un réseau en fonctionnement	

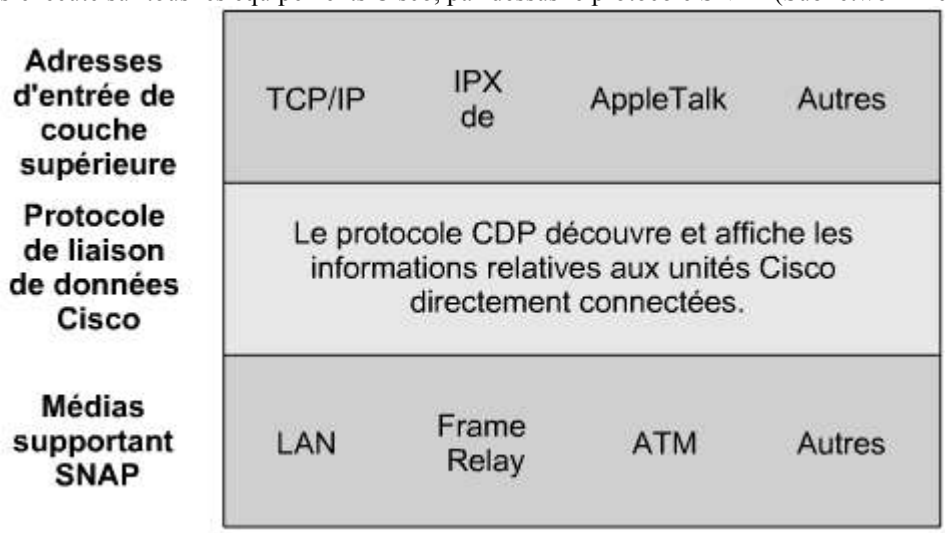
Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
• Utilisation d'un sous-ensemble de commandes Cisco IOS pour analyser et signaler les problèmes sur le réseau • Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	• Etablissement de communication entre un équipement terminal et l'IOS du routeur, et utilisation de l'IOS en vue de l'analyse du système • Utilisation des commandes intégrées à l'IOS pour analyser et signaler les problèmes sur le réseau • Découverte et analyse du voisinage réseau depuis le routeur via la fonctionnalité de couche liaison de données intégrée • Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	

4.1 Découverte et connexion aux équipements voisins

4.1.1 Introduction au protocole CDP

CDP (Cisco Discovery Protocol) est un protocole de couche 2 qui relie des médias physiques de niveau inférieur et des protocoles de couche réseau de niveau supérieur, comme l'illustre la figure 1. CDP permet d'obtenir des informations sur les équipements voisins, comme leurs types, les interfaces du routeur auxquelles ils sont connectés, les interfaces utilisées pour établir les connexions, ainsi que leurs numéros de modèle. CDP est indépendant du média comme du protocole, et il s'exécute sur tous les équipements Cisco, par-dessus le protocole SNAP (Subnetwork Access Protocol).



CDP Version 2 (CDPv2) est la version la plus récente de ce protocole. Cisco IOS (Version 12.0(3)T ou ultérieure) prend en charge CDPv2. CDP Version 1 (CDPv1) est activé par défaut avec la plate-forme logicielle Cisco IOS (Version 10.3 à 12.0(3)T).

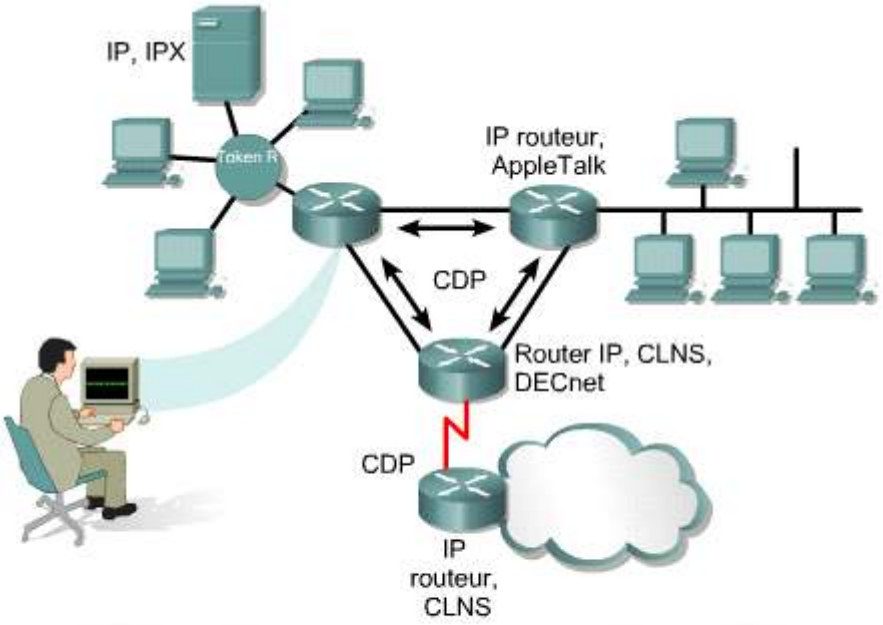
Lors du démarrage d'un équipement Cisco, CDP démarre de façon automatique et permet à l'équipement de détecter les équipements voisins qui exécutent comme lui ce protocole. CDP s'exécute sur la couche liaison de données et permet à deux systèmes de se découvrir, même s'ils utilisent des protocoles de couche réseau différents.

Chaque équipement configuré pour CDP envoie périodiquement des messages, appelés annonces, aux équipements réseau directement connectés. Chaque équipement annonce au moins une adresse à laquelle il peut recevoir des messages SNMP (Simple Network Management Protocol). Les annonces contiennent également des informations de « durée de vie » ou durée de conservation, indiquant pendant combien de temps les équipements récepteurs doivent conserver les informations CDP avant de les éliminer. De plus, chaque équipement écoute les messages CDP périodiques envoyés par les autres équipements afin d'identifier ceux qui se trouvent dans le voisinage.

4.1 Découverte et connexion aux équipements voisins

4.1.2 Informations obtenues avec CDP

CDP sert principalement à découvrir tous les équipements Cisco qui sont directement connectés à un équipement local. Exécutez la commande **`show cdp neighbors`** pour afficher les mises à jour CDP sur l'équipement local.



Une commande unique récapitule les protocoles et les adresses sur la cible (par exemple, un routeur Cisco voisin).

La figure 1 illustre la façon dont le protocole CDP transmet à l'administrateur réseau les données recueillies. Tous les routeurs exécutant le protocole CDP partagent avec leurs voisins des informations protocolaires. L'administrateur réseau peut visualiser les résultats de cet échange d'informations via CDP sur une console reliée à un routeur local.

L'administrateur utilise la commande **`show cdp neighbors`** pour afficher les informations sur les réseaux directement connectés au routeur. CDP fournit des informations sur chaque équipement CDP voisin en transmettant des TLV (*Type Length Value*), c'est-à-dire des blocs d'informations incorporés dans des annonces CDP.

Les TLV d'équipement affichées par les commandes **`show cdp neighbors`** sont notamment:

- l'identifiant,
- l'interface locale,
- la durée de conservation,
- la capacité,
- la plate-forme,

- l'ID du port.

Les TLV suivantes ne sont comprises que dans CDPv2:

- le nom de domaine de gestion VTP,
- le VLAN natif,
- le mode Full-Duplex ou Half-Duplex.

Remarquez que le routeur situé au niveau le plus bas sur la figure n'est pas directement connecté au routeur de la console de l'administrateur. Pour obtenir des informations CDP sur cet équipement, l'administrateur doit établir une session telnet avec un routeur qui lui est directement connecté.

4.1 Découverte et connexion aux équipements voisins

4.1.3 Mise en oeuvre, surveillance et maintenance du protocole CDP

Les commandes suivantes sont utilisées pour mettre en oeuvre, surveiller et mettre à jour les informations CDP: 1

Commande	Mode	Usage
`cdp run`	Mode de configuration globale	Active CDP globalement sur le routeur.
`cdp enable`	Mode de configuration d'interface	Active CDP sur une interface.
`clear cdp counters`	Mode privilégié	Remet à zéro les compteurs de trafic.
`show cdp`	Mode utilisateur ou privilégié	Indique l'intervalle entre les transmissions des annonces CDP, la durée de validité d'une annonce CDP pour un port donné (en secondes) et la version de l'annonce.
`show cdp entry {* | device-name [*] [protocol | version]}`	Mode utilisateur ou privilégié	Affiche les informations relatives à un voisin spécifique. L'affichage peut être limité aux informations de version ou de protocole.
`show cdp interface [type number]`	Mode utilisateur ou privilégié	Affiche les informations relatives aux interfaces sur lesquelles le protocole CDP est active.
`show cdp neighbors [type number] [detail]`	Mode utilisateur ou privilégié	Indique le type et le nom de l'unité détectée, le numéro et le type de l'interface locale (port), la durée de validité de l'annonce CDP pour le port (en secondes), le numéro de produit de l'unité et l'ID du port. L'utilisation du mot-clé " detail " permet d'afficher des informations sur l'ID du VLAN natif, le mode duplex et le nom de domaine VTP associé aux unités voisines.

- **`cdp run`**
- **`cdp enable`**
- **`show cdp traffic`**
- **`clear cdp counters`** 2

Router

```
Rtl#show cdp traffic
CDP counters:
     Total packets output: 6, Input:6
     Hdrsyntax: 0, Chksum error: 0, Encaps failed:0
     No memory: 0, Invalid packet: 0, Fragmented:0
     CDP version1 advertisements output: 0, Input:0
     CDP version2 advertisements output: 6, Input:6
Rtl#clear cdp counters
Rtl#show cdp traffic
CDP counters:
     Total packets output: 0, Input:0
     Hdrsyntax: 0, Chksum error: 0, Encaps failed:0
     No memory: 0, Invalid packet: 0, Fragmented:0
     CDP version1 advertisements output: 0, Input:0
     CDP version2 advertisements output: 0, Input:0
Rtl#
```

- **show cdp** 3

Router

```
CDP Version 1
Rt3#show cdp
Global CDP information:
   Sending CDP packets every 60 seconds
   Sending a holdtime value of 180 seconds
Rt3#
CDP Version 2
Rtl#show cdp
Global CDP information
   Sending CDP packets every 60 seconds
   Sending a holdtime value of 180 seconds
   Sending CDPv2 advertisments is enabled
Rtl#
```

- **show cdp entry {*|*nom-équipement*[*][protocol | version]}** 4

Router

```
Rtl#show cdp entry Rt2
-------------------
Device ID: Rt2
Entry address(es):
IP address: 192.168.2.2
Platform: cisco 2621, Capabilities: Router
Interface: Serial0/0, PortID(outgoing port): Serial0/0
Holdtime: 139 sec

Version:
Cisco Internetwork Operating System Software
IOS (tm)C2600 Software(C2600-DO3S-M), Version 12.0(5)TI,
RELEASE
SOFTWARE(fc1)
Copyright(c) 1986-1999 by cisco System, Inc.
Compiled Tue 17-Aug-99 13:18 bycmong

advertisement version:2
Rtl#
```

- **show cdp interface [type number]** 5

Router

```
Rtl#show cdp interface serial0/0
Serial0/0 is up, line protocol is up
   Encapsulation HDLC
   Sending CDP packets every 60 seconds
   Holdtime is 180 seconds

Rtl#show cdp interface fastethernet0/0
FastEthernet0/0 is up, line protocol is up
   Encapsulation ARPA
   Sending CDP packets every 60 seconds
   Holdtime is 180 seconds
Rtl#
```

- **show cdp neighbors [type number] [detail]** 6

Router

```
Rt2#show cdp neighbors
Capability Codes: R-Router, T-Trans Bridge, B-Source
Route Bridge, S-Switch, H-Host, I-IGMP, r-Repeater

DeviceID Local Intrfce Holdtme Capablty Platform  Port ID
Rt3      Ser0/1        152     R        2500      Ser1
Rtl      Ser0/0        121     R        2620      Ser0/0
Rt2#
```

La commande **cdp run** est utilisée pour activer CDP de façon globale sur le routeur. Par défaut, ce protocole est activé globalement. La commande **cdp enable** est utilisée pour activer CDP sur une interface particulière. Sur la version 10.3 de la plate-forme logicielle Cisco IOS, CDP est activé par défaut sur toutes les interfaces prises en charge pour envoyer et recevoir des informations CDP. CDP pourrait être activé sur chacune des interfaces des équipements à l'aide de la commande **cdp enable**.

Activité de TP

Activité en ligne : Mise en oeuvre, surveillance et maintenance du protocole CDP

Au cours de ce TP, les étudiants vont apprendre certaines des commandes associées au protocole CDP (Cisco Discovery Protocol), ainsi qu'à afficher certaines informations CDP.

4.1 Découverte et connexion aux équipements voisins

4.1.4 Création d'un schéma de réseau de l'environnement

Le protocole CDP est un protocole simple ne surchargeant pas les réseaux. Une trame CDP peut être de petite taille mais fournir de nombreuses informations utiles sur les équipements Cisco voisins connectés.

Ces informations peuvent être utilisées pour créer un schéma de réseau des équipements connectés. Les équipements connectés aux équipements voisins peuvent être découverts à l'aide de Telnet, puis en utilisant la commande **show cdp neighbors**.

Rt2

```
Rt2#show cdp neighbors
Capability Codes: R-Router, T-Trans Bridge, B-Source
Route Bridge, S-Switch, H-Host, I-IGMP, r-Repeater

DeviceID Local Intrfce Holdtme Capablty Platform  Port ID
Rt3      Ser0/1        152     R        2500      Ser1
Rt1      Ser0/0        121     R        2620      Ser0/0
Rt2#
```

Activité de TP

Exercice : Création d'un schéma de réseau à l'aide de CDP

Au cours de ce TP, les étudiants vont utiliser les commandes CDP pour obtenir des informations sur les équipements réseau voisins

4.1 Découverte et connexion aux équipements voisins

4.1.5 Désactivation du protocole CDP

Pour désactiver CDP au niveau global, exécutez la commande **no CDP run** en mode de configuration globale. 1 Si CDP est désactivé de façon globale, il est impossible d'activer des interfaces individuelles pour ce protocole.

Rt1

```
Rtl#show cdp
Global CDP information
   Sending CDP packets every 60 seconds
   Sending a holdtime value of 180 seconds
   Sending CDPv2 advertisements is enabled
Rtl#configure terminal
Enter configuration commands, one per line. End with
 CNTL/Z
Rtl(config)#no cdp run
Rtl(config)#^Z
Rtl#show cdp
%CDP is not enabled
Rtl#configure terminal
Enter configuration commands, one per line. End with
 CNTL/Z
Rtl(config)#cdp run
Rtl(config)#^Z
Rtl#show cdp
Global CDP information:
   Sending CDP packets every 60 seconds
   Sending a holdtime value of 180 seconds
   Sending CDPv2 advertisements is enabled
Rtl#
```

Sur la version 10.3 de la plate-forme logicielle Cisco IOS, CDP est activé par défaut sur toutes les interfaces prises en charge pour envoyer et recevoir des informations CDP. Toutefois, sur certaines interfaces, telles que les interfaces asynchrones, CDP est désactivé par défaut. Si CDP est désactivé, utilisez la commande **`CDP enable`** en mode de configuration d'interface. Pour désactiver CDP sur une interface spécifique une fois qu'il a été activé, utilisez la commande **`no CDP enable`** en mode de configuration d'interface.

4.1 Découverte et connexion aux équipements voisins

4.1.6 Dépannage du protocole CDP

Vous pouvez utiliser les commandes suivantes pour afficher la version, les informations de mise à jour, les tables et le trafic:
1

Commande	Description
clear cdp table	Supprime la table d'informations CDP relative aux unités voisines.
clear cdp counters	Remet à zéro les compteurs de trafic.
show cdp traffic	Affiche les compteurs CDP, notamment le nombre de paquets envoyés et reçus, ainsi que les erreurs de somme de contrôle.
show debugging	Affiche l'information concernant les types de débogage qui sont présentement actifs.
debug cdp adjacency	Informations CDP sur les unités voisines
debug cdp events	Événements CDP
debug cdp ip	Informations IP CDP
debug cdp packets	CDP packet-related information
cdp timer	Indique la fréquence d'envoi de mises à jour CDP par la plate-forme logicielle Cisco IOS.
cdp holdtime	Indique le délai de conservation à envoyer dans le paquet de mises à jour CDP.
show cdp	Affiche des informations CDP globales, notamment sur les compteurs et les délais de conservation.

- **clear cdp table**
- **clear cdp counters**
- **show cdp traffic** 2

Rt2

```
Rt2#show cdp traffic
CDP counters:
   Total packets output: 526, Input: 323
   Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
   No memory: 0, Invalid packet: 0, Fragmented: 0
   CDP version 1 advertisements output: 168, Input: 153
   CDP version 2 advertisements output: 358, Input: 170
```

- **show debugging**
- **debug cdp adjacency**
- **debug cdp events**
- **debug cdp ip**
- **debug cdp packets**
- **cdp timer**
- **cdp holdtime**
- **show cdp**

Activité de TP

Exercice : Utilisation des commandes CDP

Au cours de ce TP, les étudiants vont utiliser les commandes CDP pour obtenir des informations sur les réseaux et les équipements voisins.

Activité de TP

Activité en ligne : Protocole ARP

Au cours de ce TP, les étudiants vont utiliser la commande **show ARP**, qui est un autre moyen d'obtenir des informations sur les équipements voisins.

Activité de TP

Activité en ligne : Voisins CDP

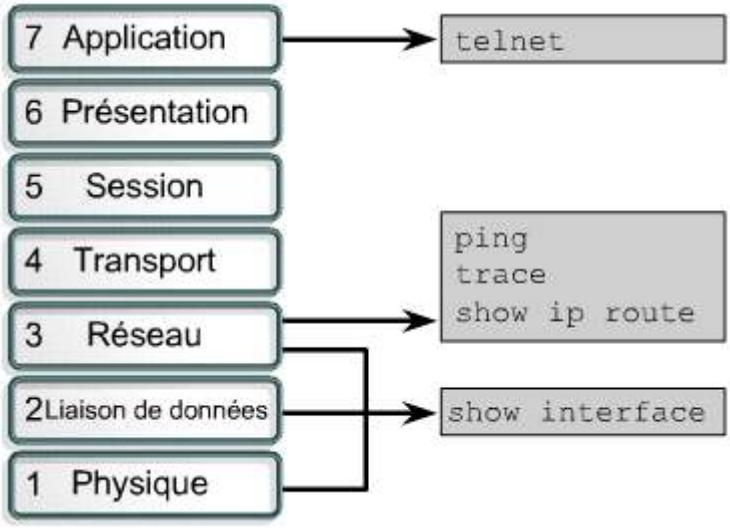
Au cours de ce TP, les étudiants vont utiliser les commandes du protocole CDP (Cisco Discovery Protocol).

4.2 Obtention d'informations sur les équipements distants

4.2.1 Telnet

Telnet est un protocole de terminal virtuel qui fait partie de la pile de protocoles TCP/IP. Il permet de se connecter à des hôtes distants. Telnet offre une capacité de terminal réseau ou de connexion à distance. Telnet est une commande EXEC de l'IOS qui permet de vérifier le logiciel de la couche application entre l'origine et la destination. Il s'agit du mécanisme de test le plus complet qui soit.

Telnet fonctionne au niveau de la couche application du modèle OSI. [1]Telnet s'appuie sur TCP afin de garantir un acheminement correct et ordonné des données entre le client et le serveur.



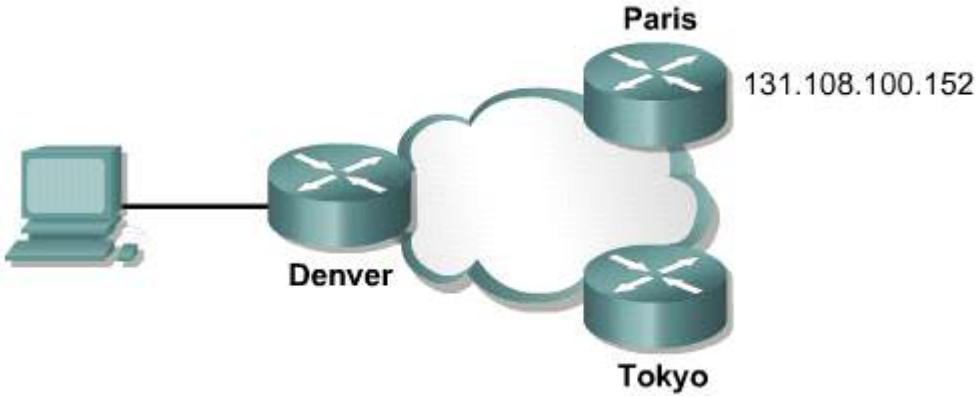
Un routeur peut établir simultanément plusieurs sessions Telnet entrantes. La plage comprise entre zéro et quatre sert à spécifier cinq lignes VTY ou Telnet. Ces cinq sessions Telnet entrantes pourraient avoir lieu en même temps.

Il est à noter que la vérification de la connectivité de la couche application est un dérivé de Telnet. La principale utilisation de Telnet est la connexion à distance aux équipements réseau. Telnet est une application simple et universelle.

4.2 Obtention d'informations sur les équipements distants

4.2.2 Établissement et vérification d'une connexion Telnet

La commande IOS EXEC de Telnet permet à un utilisateur d'envoyer une requête Telnet d'un équipement Cisco à une autre équipement. Avec l'implémentation Cisco du protocole TCP/IP, il n'est pas nécessaire d'entrer la commande **connect** ou **telnet** pour établir une connexion Telnet. Vous pouvez entrer le nom d'hôte ou l'adresse IP du routeur. Pour mettre fin à une session Telnet, utilisez les commande EXEC **exit** ou **logout**. [1]



Lancer une session:

```
Denver>telnet paris
```

Mettre fin à une session

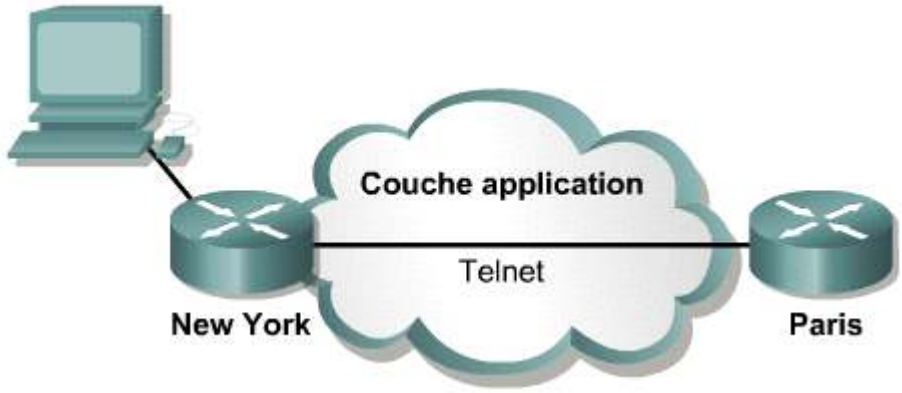
```
Paris>exit
```

Pour lancer une session Telnet, n'importe laquelle des alternatives suivantes peut être utilisée:

```
Denver>connect paris
Denver>paris
Denver>131.108.100.152
Denver>telnet paris
```

Un nom ne peut fonctionner qu'en présence d'une table de noms d'hôtes ou d'un accès à DNS pour Telnet. Sinon, vous devez entrer l'adresse IP du routeur distant.

À l'aide de Telnet, vous pouvez effectuer un test afin de déterminer s'il est possible ou non d'accéder à un routeur distant. Comme l'illustre la figure 2, si vous réussissez à connecter le routeur de York au routeur de Paris via Telnet, vous avez effectué un test de base de la connexion réseau. Cette opération peut être exécutée en mode utilisateur ou en mode privilégié.



S'il est possible d'obtenir l'accès distant via un autre routeur, alors au moins une application TCP/IP peut atteindre le routeur distant. Une connexion Telnet réussie indique que l'application de couche supérieure fonctionne correctement.

Si vous pouvez établir une connexion Telnet avec un routeur, mais pas avec un autre, l'échec de Telnet est vraisemblablement dû à des problèmes spécifiques d'adressage, d'attribution de noms ou d'autorisation d'accès. Ces problèmes peuvent exister sur votre routeur ou sur celui que vous avez tenté d'atteindre via Telnet. Dans ce cas, essayez d'exécuter la commande **`ping`**, traitée plus loin dans cette section. La commande **`ping`** permet de tester de bout en bout les connexions sur la couche réseau.

Une fois la requête Telnet terminée, déconnectez-vous de l'hôte. La connexion Telnet se termine après dix minutes d'inactivité par défaut, ou si vous entrez la commande **`exit`** à l'invite de commande.

Activité de TP

Exercice : Établissement et vérification d'une connexion Telnet

Au cours de ce TP, les étudiants vont établir une connexion Telnet avec un routeur distant et vérifier que la couche application entre l'origine et la destination fonctionne correctement.

4.2 Obtention d'informations sur les équipements distants

4.2.3 Déconnexion et interruption de sessions Telnet

L'une des principales fonctions de la commande **telnet** est la commande d'interruption. Cependant, il existe un problème potentiel lorsqu'une session Telnet est interrompue alors que vous appuyez sur la touche **Entrée**. La plate-forme logicielle Cisco IOS reprend la dernière connexion Telnet interrompue. La touche **Entrée** est fréquemment utilisée. Avec une session Telnet interrompue, il est possible de se reconnecter à un autre routeur. Cela est risqué si des modifications sont apportées à la configuration ou si des commandes EXEC sont utilisées. Soyez particulièrement attentif au routeur qui est utilisé lorsque vous utilisez la fonction Telnet interrompue.

Une session est interrompue pendant une durée limitée. Pour reprendre une session Telnet interrompue, il vous suffit d'appuyer sur **Entrée**. La commande **show sessions** indique les sessions Telnet actives.

La procédure de déconnexion d'une session Telnet est la suivante:

- Entrez la commande **disconnect**
- À la suite de la commande, entrez le nom ou l'adresse IP du routeur. Exemple:

```
Denver>disconnect paris
```

Pour interrompre une session Telnet, procédez comme suit:

- Appuyez sur **Ctrl-Shift-6,** puis sur **x**
- Entrez le nom du routeur ou son adresse IP

Lancer une session

```
Denver>telnet paris
```

Mettre fin à une session

```
Paris>exit
```

Interrompre une session

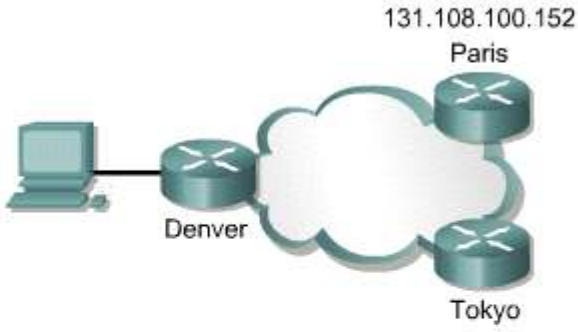
```
Paris><Ctrl><Shift><6><x>
Denver>
```

Reprendre une session

```
Denver><Return>
```

Se déconnecter d'une session

```
Denver>disconnect paris
```



Afficher les sessions

```
Denver#show sessions
 Conn    Host    Address            Idle    Conn Name
 1       Paris   131.108.100.152    0       Paris
 2       Tokyo   126.102.57.63      0       Tokyo
```

Activité de TP

Exercice : Interruption et déconnexion de sessions Telnet

Au cours de ce TP, les étudiants vont établir une session Telnet avec un routeur distant, puis interrompre et rétablir cette session.

4.2 Obtention d'informations sur les équipements distants

4.2.4 Utilisation avancée de Telnet

Plusieurs sessions Telnet peuvent être ouvertes simultanément. L'utilisateur peut alors permuter entre les deux sessions. Le nombre de sessions ouvertes simultanément est défini par la commande **`session limit`**.

Pour permuter entre sessions en quittant une session et en reprenant une session ouverte précédemment, utilisez les commandes illustrées dans la figure 1

Commande	Usage
`Ctrl-Shift-6` then **`x`**	Quitte la session actuelle et revient à l'invite EXEC.
`Resume`	Rétablit la connexion.

.

Une nouvelle connexion peut être établie à l'invite EXEC.

Plusieurs sessions Telnet peuvent être utilisées et interrompues à l'aide de la séquences **Ctrl-Shift-6**, puis **x**. La session peut être reprise à l'aide de la touche **Entrée**. Si vous utilisez cette touche, la plate-forme logicielles Cisco IOS reprend la connexion à la dernière connexion Telnet interrompue. Si elle est utilisée, la commande **`resume`** requiert un identifiant de connexion. Vous pouvez afficher ce dernier à l'aide de la commande **`show sessions`**. 2

Router

```
Denver>telnet Paris
Trying Paris (131.108.100.152)…Open
User Access Verification
Password:  xxxxx
Paris>    (User pressed Ctrl-Shift- 6, then x)
Denver>telnet Tokyo
Trying Tokyo (127.102.57.63)…..Open
User Access Verification
Password: xxxxx
Tokyo>    (User pressed Ctrl-Shift-6, then x)
Denver>show sessions
Conn Host Address            Idle     Conn Name
  1  131.108.100.152           0        Paris
  2  127.102.57.63             0        Tokyo
```

Activité de TP

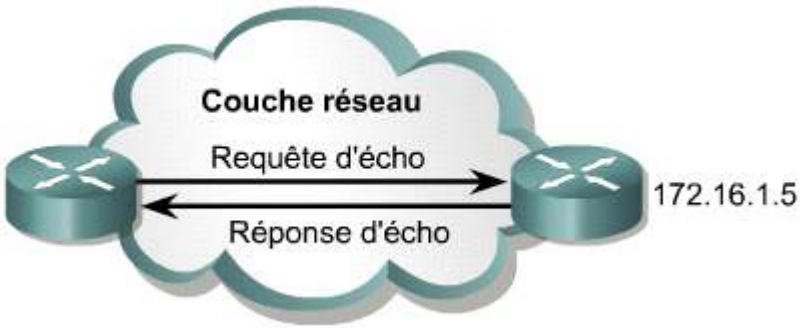
Exercice : Opérations Telnet avancées

L'objectif de ce TP est d'utiliser la commande telnet pour accéder à distance à d'autres routeurs.

4.2 Obtention d'informations sur les équipements distants

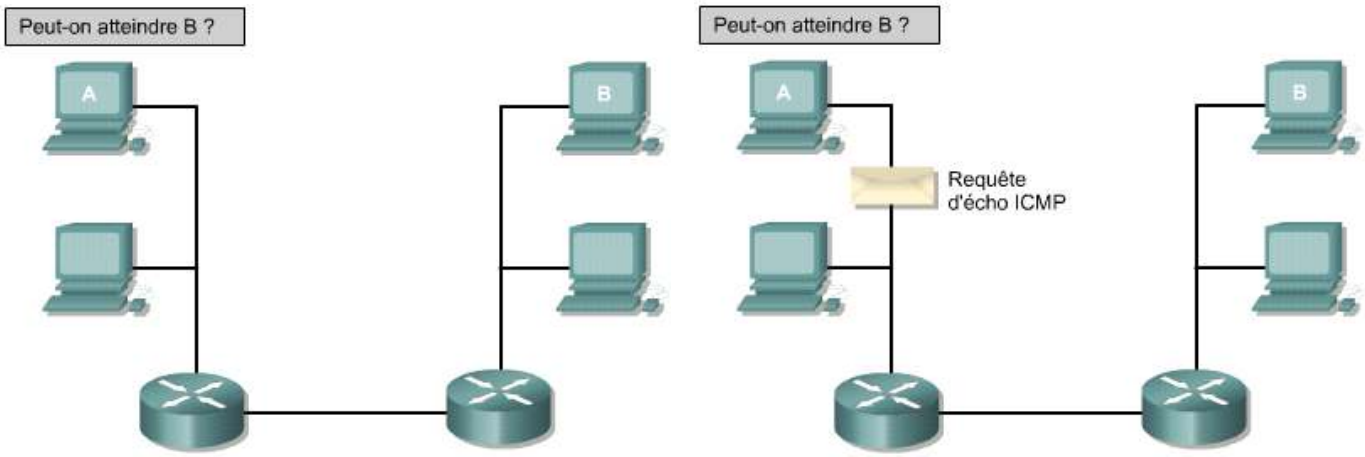
4.2.5 Tests de connectivité alternative

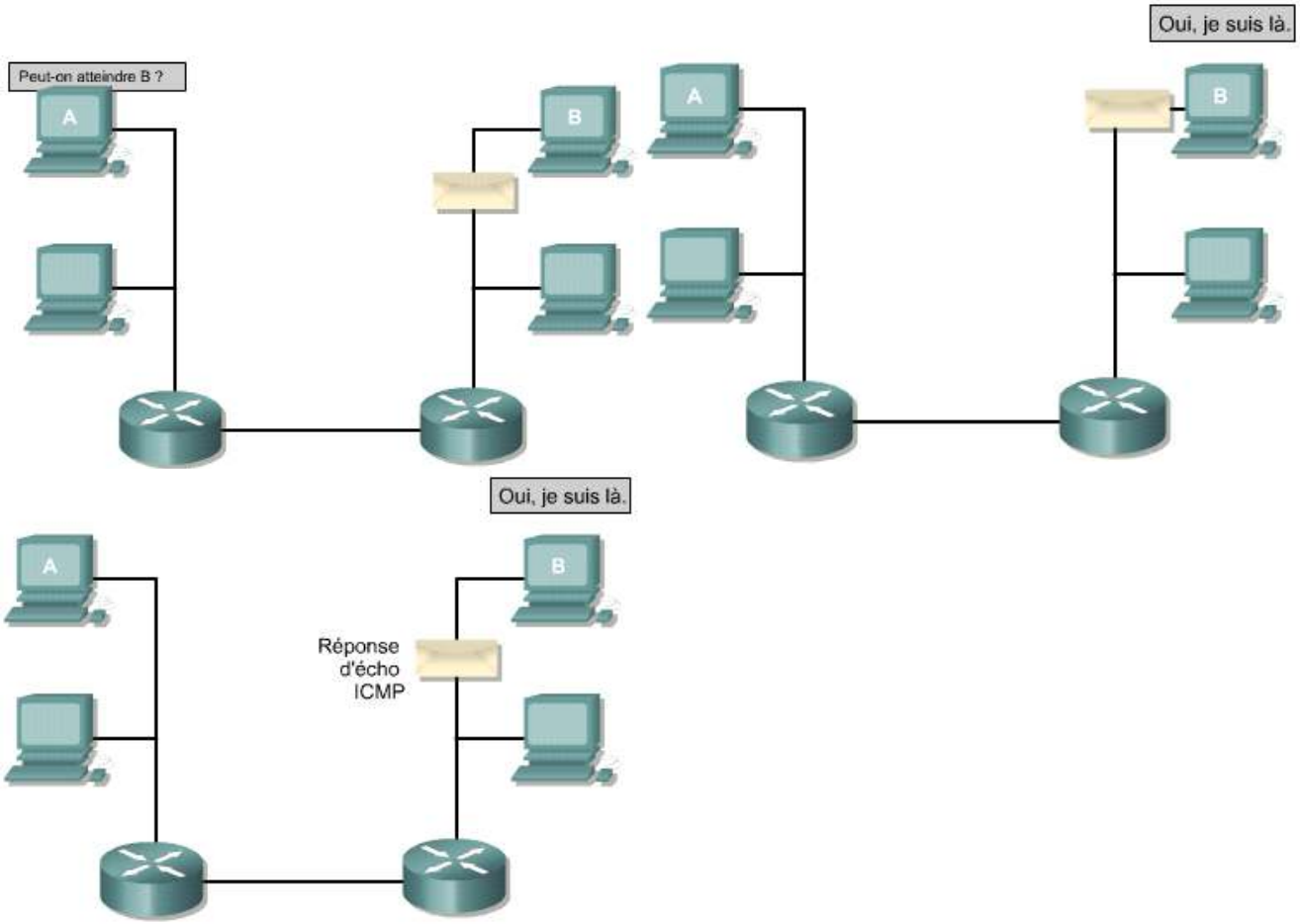
Un grand nombre de protocoles réseau prennent en charge un protocole d'écho qui contribue à faciliter le diagnostic de la connectivité de base d'un réseau. Les protocoles d'écho permettent de vérifier si les paquets de protocole sont en cours d'acheminement. La commande **ping** envoie un paquet à l'hôte de destination et attend un paquet de réponse de celui-ci. Les résultats du protocole d'écho peuvent aider à évaluer la fiabilité chemin-hôte et les délais sur le chemin. Ils permettent aussi de déterminer si l'accès à l'hôte est possible et si ce dernier fonctionne. Il s'agit d'un mécanisme de test des plus élémentaires. Cette opération peut être exécutée en mode utilisateur ou en mode privilégié.




```
Router>ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>
```

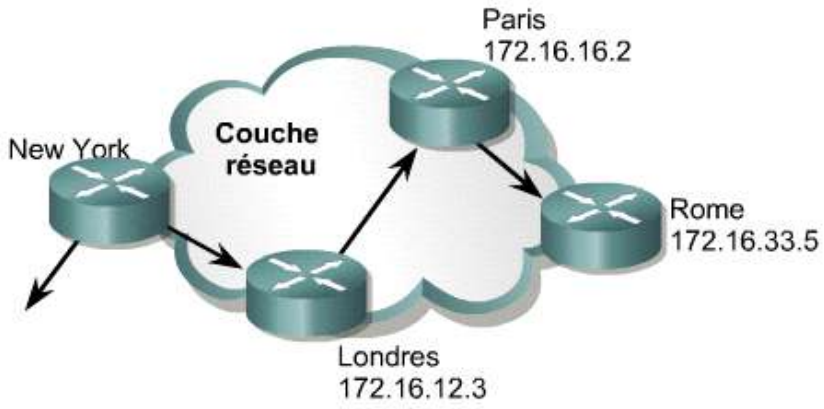
La cible de la commande ping 172.16.1.5 de la figure 1 a répondu aux cinq datagrammes envoyés. Les points d'exclamation (!) indiquent chaque écho réussi. Si votre écran affiche un ou plusieurs points (.) au lieu de points d'exclamation, cela signifie que l'application de votre routeur a été temporisée pendant qu'elle attendait un paquet d'écho de la cible précisée dans la commande ping. La commande utilisateur **ping** permet de diagnostiquer la connectivité de base d'un réseau. Elle utilise le protocole ICMP (Internet Control Message Protocol). 2





La commande traceroute constitue l'outil idéal pour rechercher la destination des données envoyées sur un réseau. Elle est semblable à la commande ping, mais au lieu de tester la connectivité de bout en bout, elle teste chaque étape de l'acheminement. Cette opération peut être exécutée en mode utilisateur ou en mode privilégié.

Dans cet exemple, le chemin entre York et Rome est analysé. Il doit passer par Londres et Paris. Si l'un de ces routeurs est inaccessible, trois astérisques s'affichent (*) à la place du nom du routeur. La commande **`traceroute`** continuera à essayer d'atteindre l'étape suivante jusqu'à ce que vous utilisiez la séquence d'échappement **Ctrl-Shift-6**.




```
York#traceroute ROME
Type escape to abort.
Tracing the route to Rome (172.16.33.5)
  1 LONDON (172.16.12.3) 8 msec 8 msec 4 msec
  2 PARIS (172.16.16.2) 8 msec 8msec 8msec
  3 ROME (172.16.33.5) 8msec 8msec 4msec

York#
```

Le test de vérification de base suivant porte également sur la couche réseau. Exécutez la commande **`show ip route`** pour déterminer s'il existe une entrée correspondant au réseau cible dans la table de routage. Cette commande sera abordée plus en détail dans un prochain module de ce cours.

La procédure d'utilisation de la commande **`ping`** est la suivante:

- **`ping`** adresse IP ou nom de destination
- appuyez sur la touche **Entrée**

La procédure d'utilisation de la commande **`traceroute`** est la suivante:

- **`traceroute`** adresse IP ou nom de destination
- appuyez sur la touche **Entrée**

Activité de TP

Exercice : Tests de connectivité – Ping

Au cours de ce TP, les étudiants vont utiliser la commande ping pour envoyer des datagrammes ICMP à un hôte cible.

Activité de TP

Exercice : Tests de connectivité – Traceroute

Au cours de ce TP, les étudiants vont utiliser la commande traceroute pour déterminer le chemin entre une origine et une destination.

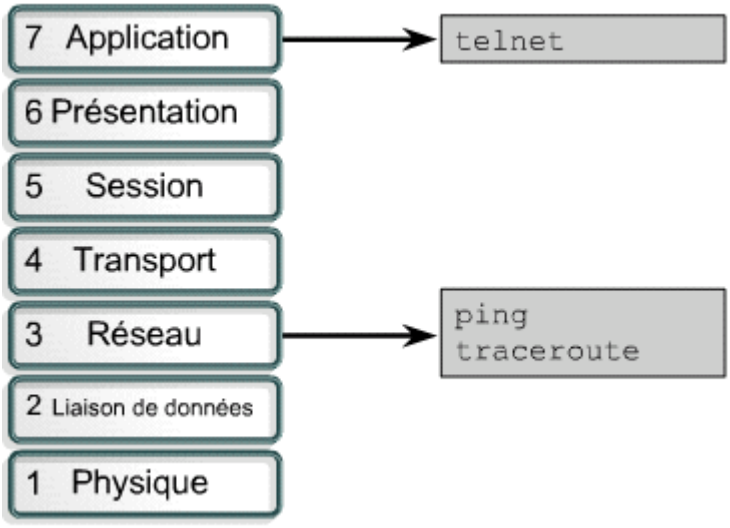
Activité de TP

Activité en ligne : Tests de connectivité alternative – Ping

Au cours de ce TP, les étudiants vont utiliser la commande ping pour envoyer des datagrammes ICMP à un hôte cible et ensuite accomplir les travaux à l'aide des informations extraites.

Les problèmes d'adressage sont les problèmes les plus fréquents sur les réseaux IP. Vous pouvez utiliser les trois commandes suivantes pour résoudre des problèmes liés aux adresses:

- **`ping`** utilise le protocole ICMP pour vérifier la connexion matérielle et l'adresse IP au niveau de la couche réseau. Il s'agit d'un mécanisme de test des plus élémentaires.
- **`telnet`** vérifie le logiciel de la couche application entre l'origine et la destination. Il s'agit du mécanisme de test le plus complet qui soit.
- **`traceroute`** permet de détecter les pannes entre les stations d'origine et de destination. Elle utilise les valeurs TTL (durée de vie) pour générer des messages à partir de chaque routeur utilisé sur le chemin.



Activité de TP

Exercice : Résolution des problèmes d'adresse IP

Au cours de ce TP, les étudiants vont configurer deux routeurs et deux stations de travail sur un petit réseau WAN.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Activation et désactivation de CDP
- Utilisation de la commande **`show cdp neighbors`**
- Identification des équipements voisins et des interfaces locales auxquels ils sont connectés
- Collecte des informations d'adresse réseau sur les équipements voisins à l'aide de CDP
- Établissement d'une connexion Telnet
- Vérification d'une connexion Telnet
- Déconnexion d'une session Telnet
- Interruption d'une session Telnet
- Exécution de tests de connectivité alternative
- Dépannage de connexions de terminal à distance

Résumé

- Le protocole CDP est un protocole de couche 2 qui relie des médias physiques de niveau inférieur et des protocoles de couche réseau de niveau supérieur.
- CDP permet d'obtenir des informations sur les unités voisines.
- Vous pouvez utiliser Telnet afin de tester l'accessibilité à partir d'un routeur distant.
- Les informations affichées par la commande ping peuvent aider à évaluer la fiabilité chemin-hôte, les délais sur le chemin, et l'accessibilité ou le fonctionnement de l'hôte.
- La commande traceroute constitue l'outil idéal pour rechercher la destination des données envoyées sur un réseau.

Vue d'ensemble

Aucun routeur Cisco ne peut fonctionner sans la plate-forme logicielle Cisco IOS (Internetwork Operating System). Chaque routeur Cisco utilise une séquence d'amorçage prédéterminée pour localiser et charger l'IOS. Ce module décrit les étapes et l'importance de cette procédure.

Les équipements réseau Cisco fonctionnent en utilisant plusieurs fichiers différents, y compris des images de l'IOS et des fichiers de configuration. Un administrateur réseau qui souhaite que son réseau fonctionne toujours sans heurt et de façon fiable doit gérer ces fichiers soigneusement de sorte que les versions appropriées soient toujours utilisées et les sauvegardes nécessaires effectuées. Ce module décrit également le système de fichiers Cisco et fournit les outils qui permettent de le gérer de façon efficace.

À la fin de ce module, les étudiants doivent être en mesure de:

- Identifier les étapes de la séquence d'amorçage d'un routeur
- Déterminer comment un équipement Cisco localise et charge l'IOS
- Utiliser la commande boot system
- Identifier les valeurs du registre de configuration
- Décrire brièvement les fichiers utilisés par l'IOS et leurs fonctions
- Lister les emplacements des différents types de fichiers sur le routeur
- Décrire brièvement les parties du nom IOS
- Enregistrer et restaurer les fichiers de configuration à l'aide de TFTP et par copier-coller
- Charger une image IOS via TFTP
- Charger une image IOS via XModem
- Vérifier le système de fichiers à l'aide des commandes show

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
5.1	Séquence de démarrage d'un routeur et vérification
5.2	Gestion du système de fichiers Cisco

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception d'un LAN simple à l'aide de la technologie Cisco • Conception d'un interréseau simple à l'aide de la technologie Cisco	• Mise en œuvre d'un LAN	• Exécution du dépannage d'un LAN simple • Dépannage d'un équipement dans un réseau en fonctionnement	

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception ou modification d'un LAN simple à l'aide de produits Cisco	• Mise en œuvre d'un LAN	• Exécution du dépannage d'un LAN et d'un VLAN • Dépannage d'un équipement dans un réseau en fonctionnement	

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
• Utilisation d'un sous-ensemble de commandes Cisco IOS pour analyser et signaler les problèmes sur le réseau • Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	• Manipulation des fichiers de configuration des équipements et de l'image système • Création d'une configuration initiale sur un routeur et enregistrement du fichier de configuration obtenu • Utilisation des commandes intégrées à l'IOS pour analyser et signaler les problèmes sur le réseau • Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur • Établissement de communication entre un équipement terminal et l'IOS du routeur, et utilisation de l'IOS en vue de l'analyse du système	• Identification et description des étapes de la séquence d'amorçage d'un routeur • Description de l'impact des commandes config-register et boot system sur la séquence d'amorçage du routeur • Description du rôle et du fonctionnement de base de la plate-forme logicielle Cisco IOS

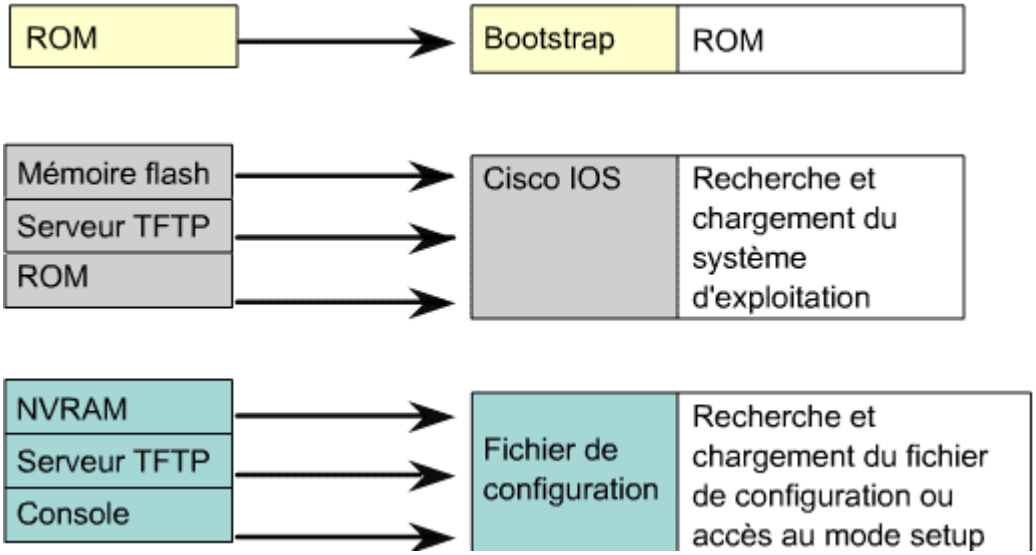
5.1 Séquence d'amorçage d'un routeur et vérification

5.1.1 Étapes de la séquence d'amorçage à la mise sous tension du routeur

L'objectif des routines de démarrage de la plate-forme logicielle Cisco IOS est de lancer les opérations de routage. Le routeur doit effectuer fiablement son travail de connexion des réseaux configurés. Pour ce faire, les routines de démarrage exécutent les opérations suivantes:

- Tester les composants matériels du routeur
- Trouver et charger l'IOS
- Rechercher et appliquer des instructions de configuration, y compris les fonctions des protocoles et les adresses des interfaces

La figure 1 illustre la séquence et les services utilisés pour initialiser le routeur.



Activité de média interactive

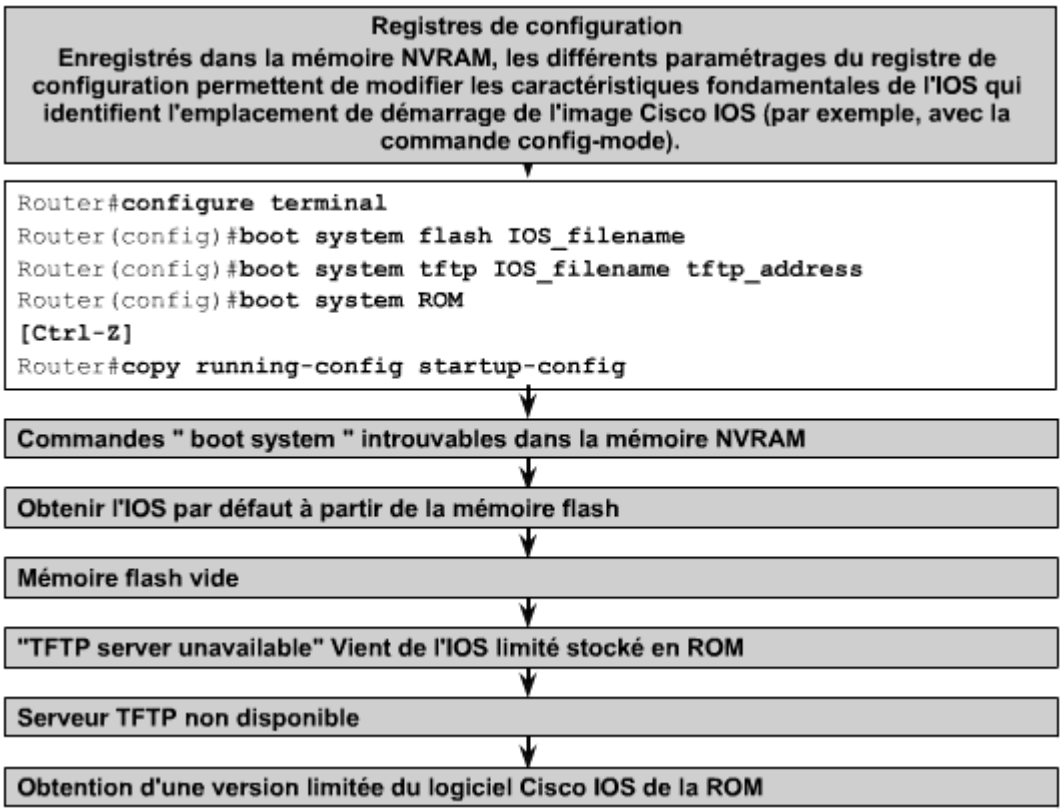
Glisser-Positionner : Séquence d'amorçage d'un routeur

À la fin de ce TP, l'étudiant sera en mesure de comprendre la séquence dans laquelle le routeur s'amorce.

5.1 Séquence d'amorçage d'un routeur et vérification

5.1.2 Comment un équipement Cisco localise et charge l'IOS

L'emplacement par défaut de la plate-forme logicielle Cisco IOS dépend de la plate-forme matérielle. En règle générale, le routeur recherche les commandes boot system enregistrées dans la mémoire NVRAM. La plate-forme logicielle Cisco IOS offre plusieurs alternatives. D'autres sources peuvent être spécifiées pour le logiciel, ou le routeur peut utiliser sa propre séquence de secours pour charger le logiciel. [1]



Les paramètres du registre de configuration (config-register) permettent les solutions alternatives suivantes:

- Vous pouvez définir des commandes boot system du mode de configuration globale pour entrer les sources de secours que le routeur utilisera dans l'ordre indiqué. Lors du redémarrage, le routeur utilisera ces commandes si nécessaire.
- Si la mémoire NVRAM ne contient pas de commandes boot system que le routeur peut utiliser, le système par défaut utilise l'IOS en mémoire flash.
- Si la mémoire flash est vide, le routeur tente d'utiliser TFTP pour charger une image IOS à partir du réseau. Le routeur utilise la valeur du registre de configuration pour créer le nom du fichier à partir duquel il amorcera une image système par défaut stockée sur un serveur du réseau.
- Si un serveur TFTP n'est pas disponible, le routeur chargera une version limitée de l'IOS de la ROM.

Activité de média interactive

Glisser-Positionner : Comment un équipement Cisco localise et charge l'IOS

À la fin de cette activité, l'étudiant sera en mesure d'identifier le processus suivi par un équipement Cisco pour trouver l'IOS au cours de l'amorçage.

5.1 Séquence d'amorçage d'un routeur et vérification

5.1.3 Utilisation de la commande boot system

Les trois exemples suivants illustrent l'utilisation de plusieurs commandes boot system pour préciser la séquence d'amorçage de secours de la plate-forme logicielle Cisco IOS. Ils présentent les entrées boot system spécifiant que l'image IOS sera d'abord chargée à partir de la mémoire flash, puis à partir d'un serveur de réseau, et enfin, à partir de la mémoire ROM.

- **Mémoire flash** – Une image système de la mémoire flash peut être chargée. Grâce à cette méthode, les informations stockées en mémoire flash ne sont pas affectées par les pannes de réseau pouvant survenir lors du chargement d'images système à partir d'un serveur TFTP. 1

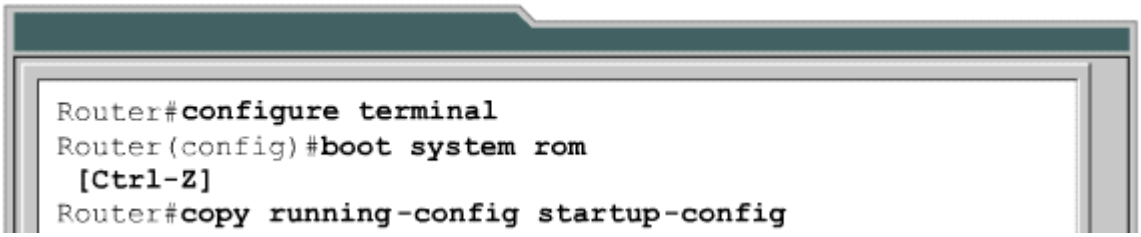
```
Router#configure terminal
Router(config)#boot system flash gsnew-image
 [Ctrl-Z]
Router#copy running-config startup-config
```

- **Serveur réseau** – Si la mémoire flash est endommagée, une image système peut être chargée à partir d'un serveur TFTP. 2

```
Router#configure terminal
Router(config)#boot system tftp IOS_image 172.16.13.111
 [Ctrl-Z]
Router#copy running-config startup-config
```

- **Mémoire ROM** – Si la mémoire flash est endommagée et que le serveur de réseau ne réussit pas à charger l'image, l'amorçage à partir de la mémoire ROM est la dernière option de bootstrap du logiciel. Toutefois, l'image système stockée en mémoire ROM ne représente qu'une partie de la plate-forme logicielle Cisco IOS (elle ne contient pas tous les protocoles, fonctions et configurations de l'IOS complet). De plus, si le logiciel a été mis à jour depuis

l'achat du routeur, la mémoire de ce dernier peut contenir une ancienne version. 3



La commande **copy running-config startup-config** enregistre les commandes dans la mémoire NVRAM. Le routeur exécutera, si nécessaire, les commandes boot system selon l'ordre dans lequel elles ont été initialement entrées en mode de configuration.

Activité de TP

Exercice : Utilisation de la commande boot system

Au cours de ce TP, les étudiants vont afficher des informations sur l'image IOS qui s'exécute sur le routeur.

Activité de TP

Activité en ligne : Préparation des commandes boot system

Au cours de ce TP, les étudiants vont afficher des informations relatives à la procédure d'amorçage du routeur, en utilisant les commandes show appropriées.

5.1 Séquence d'amorçage d'un routeur et vérification

5.1.4 Registre de configuration

L'ordre suivant lequel le routeur cherche les informations de bootstrap est déterminé par la valeur du champ d'amorçage du registre de configuration. Le paramètre du registre de configuration par défaut peut être modifié à l'aide de la commande de configuration globale **config-register**. Utilisez un nombre hexadécimal comme argument pour cette commande.

```
Router#show version
Cisco Internetwork Operating System Software  IOS
(tm) 2500 Software (C2500-JS-L), Version 12.1(5),
RELEASE SOFTWARE (fc1) Copyright (c) 1986-2000 by
cisco Systems, Inc. Compiled Wed 25-Oct-00 05:18
by cmong Image text-base: 0x03071DB0, data-base:
0x00001000
ROM: System Bootstrap, Version 5.2(8a), RELEASE
SOFTWARE BOOTFLASH: 3000 Bootstrap Software (IGS-
RXBOOT), Version 10.2(8a), RELEASE SOFTWARE (fc1)
Router uptime is 7 minutes System returned to ROM
by reload System image file is "flash:c2500-js-
l_121-5.bin".
cisco 2500 (68030) processor (revision D) with
16384K/2048K bytes of memory. Processor board ID
03867477, with hardware revision 00000000 Bridging
software. X.25 software, Version 3.0.0. SuperLAT
software (copyright 1990 by Meridian Technology
Corp). TN3270 Emulation software. 1 Token
Ring/IEEE 802.5 interface(s) 2 Serial network
interface(s) 32K bytes of non-volatile
configuration memory. 16384K bytes of processor
board System flash (Read ONLY)
Configuration register is 0x2142
```

Le registre de configuration est un registre de 16 bits qui se trouve dans la mémoire NVRAM. Les quatre derniers bits du registre de configuration forment le champ d'amorçage. Pour que les 12 bits supérieurs ne soient pas modifiés, extrayez d'abord les valeurs en cours du registre de configuration à l'aide de la commande **`show version`**. 1 Utilisez ensuite la commande **`config-register`**, en modifiant uniquement la valeur du dernier chiffre hexadécimal.

Pour modifier le champ d'amorçage dans le registre de configuration, suivez ces directives: 2

Valeur	Description
0xnnn0	Utilisation du mode moniteur ROM (démarrage manuel à l'aide de la commande **`b`**)
0xnnn1	Amorce la première image dans la flash. Cependant, sur des plateformes plus anciennes, l'amorçage se fera sur une version de l'IOS plus ancienne située dans la ROM
0xnnn2 à 0xnnnF	Recherche des commandes "**`boot system`**" dans la mémoire NVRAM (0xnnn2 est la valeur par défaut si le routeur a une mémoire flash)"

- Pour passer en mode moniteur ROM, attribuez la valeur 0x*nnn*0 au registre de configuration, où *nnn* représente la valeur précédente des chiffres non liés au champ d'amorçage. Cette valeur définit les bits du champ d'amorçage à la valeur binaire 0000. À partir de ce mode, amorcez le système d'exploitation manuellement en entrant la commande **`b`** à l'invite du mode
- Pour démarrer à partir de la première image de la flash ou démarrer à partir de l'IOS dans la ROM (dépendant de la plateforme), réglez le registre de configuration à 0xnnn1, ou nnn est la valeur précédente des bits qui ne faisait pas partie du champ d'amorçage. Cette valeur règle les bits du champ d'amorçage à la valeur binaire 0001. Les plateformes plus anciennes, telles que Cisco 1600 et 2500, s'amorceront sur une version limitée de l'IOS Cisco située dans la ROM. Les versions plus récentes, telles que Cisco 1700, 2600 et les routeurs de haut de gamme s'amorceront à partir de la première image de la flash

- Pour configurer le système pour qu'il utilise les commandes boot system de la NVRAM, attribuez la valeur 0x*nnn*1 au registre de configuration, où *nnn* représente la valeur précédente des chiffres non liés au champ d'amorçage. Ces valeurs définissent les bits du champ d'amorçage à une valeur binaire comprise entre 0010 et 1111. L'utilisation des commandes boot system en mémoire NVRAM est l'option par défaut.

Activité de TP

Activité en ligne : Registre de configuration

Au cours de ce TP, les étudiants vont apprendre à modifier la procédure d'amorçage d'un routeur.

5.1 Séquence d'amorçage d'un routeur et vérification

5.1.5 Dépannage d'une panne d'amorçage de l'IOS

Plusieurs éléments peuvent être à l'origine du mauvais amorçage d'un routeur:

- le fichier de configuration comporte une instruction **`boot system`** manquante ou incorrecte,
- une valeur du registre de configuration est incorrecte,
- l'image flash est corrompue,
- une panne matérielle.

Lors de son amorçage, le routeur recherche une instruction **`boot system`** dans le fichier de configuration. Cette instruction peut forcer le routeur à s'amorcer à partir d'une image autre que celle de l'IOS en mémoire flash. Pour identifier la source de l'image d'amorçage, tapez la commande **`show version`** et cherchez la ligne qui identifie la source de l'image d'amorçage.

1

```
Router#show version
Cisco Internetwork Operating System Software  IOS
(tm) 2500 Software (C2500-JS-L), Version 12.1(5),
RELEASE SOFTWARE (fc1) Copyright (c) 1986-2000 by
cisco Systems, Inc. Compiled Wed 25-Oct-00 05:18
by cmong Image text-base: 0x03071DB0, data-base:
0x00001000
ROM: System Bootstrap, Version 5.2(8a), RELEASE
SOFTWARE BOOTFLASH: 3000 Bootstrap Software (IGS-
RXBOOT), Version 10.2(8a), RELEASE SOFTWARE (fc1)
Router uptime is 7 minutes System returned to ROM
by reload System image file is "flash:c2500-js-
l_121-5.bin"
cisco 2500 (68030) processor (revision D) with
16384K/2048K bytes of memory. Processor board ID
03867477, with hardware revision 00000000 Bridging
software. X.25 software, Version 3.0.0. SuperLAT
software (copyright 1990 by Meridian Technology
Corp). TN3270 Emulation software. 1 Token
Ring/IEEE 802.5 interface(s) 2 Serial network
interface(s) 32K bytes of non-volatile
configuration memory. 16384K bytes of processor
board System flash (Read ONLY)
Configuration register is 0x2142
```

Utilisez la commande **show running-config** et recherchez une instruction **boot system** au début de la configuration. Si l'instruction **boot system** désigne une image IOS incorrecte, supprimez cette instruction à l'aide de la forme no de la commande.

Un paramètre de registre de configuration incorrect empêchera l'IOS de se charger à partir de la mémoire flash. La valeur du registre de configuration indique au routeur où obtenir l'IOS. Cela peut être confirmé à l'aide de la commande **show version** et en examinant la dernière ligne du registre de configuration. La valeur correcte varie selon chaque plate-forme matérielle. À des fins de référence, vous pouvez imprimer les informations affichées par la commande **show version**. Si la documentation de l'interréseau n'est pas disponible, vous trouverez des ressources sur le CD de la documentation Cisco ou sur le site Web de Cisco pour identifier la valeur de registre de configuration correcte. Corrigez la valeur en modifiant le registre de configuration et en l'enregistrant en tant que configuration de démarrage.

Si le problème persiste, il se peut que le fichier d'image flash du routeur soit corrompu. Dans ce cas, un message d'erreur doit s'afficher lors de l'amorçage. Ce message peut avoir plusieurs formes. Exemples :

- open: read error...requested 0x4 bytes, got 0x0
- trouble reading device magic number
- boot: cannot open "flash:"
- boot: cannot determine first file name on device "flash:"

Si l'image flash est corrompue, une nouvel IOS doit être chargé dans le routeur.

Si aucun des éléments précédents ne semble être à l'origine du problème, le routeur présente peut-être une panne matérielle. Dans ce cas, contactez le centre d'assistance technique de Cisco (TAC) On n'est jamais totalement à l'abri d'une défaillance matérielle.

REMARQUE:
Les commandes **show running-config** ou **show startup-config** n'affichent pas la valeur du registre de configuration.

Activité de TP

Exercice : Dépannage des problèmes d'amorçage du registre de configuration

Au cours de ce TP, les étudiants vont vérifier et documenter les paramètres du registre de configuration relatifs à la méthode d'amorçage.

Activité de TP

Activité en ligne : Dépannage d'une panne d'amorçage de l'IOS

Au cours de ce TP, les étudiants vont vérifier et documenter les paramètres du registre de configuration relatifs à la méthode d'amorçage, configurer ensuite le routeur pour qu'il s'amorce à partir de la mémoire NVRAM et enfin recharger le routeur.

5.2 Gestion du système de fichiers Cisco

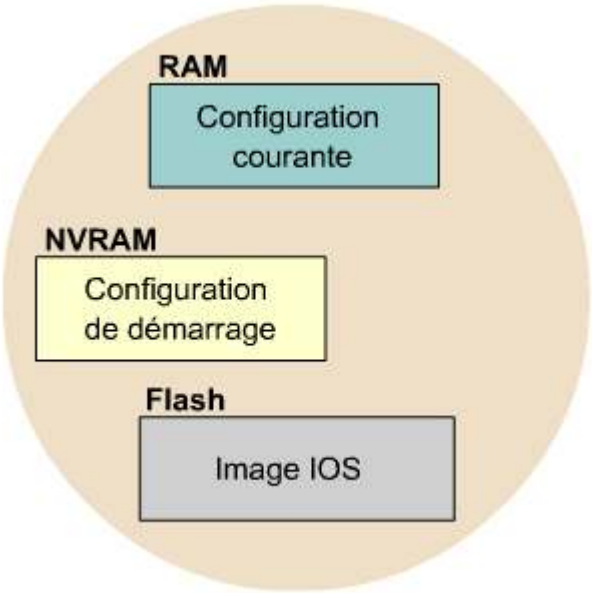
5.2.1 Vue d'ensemble du système de fichiers IOS

Les routeurs et commutateurs ne peuvent fonctionner sans logiciel. Les deux types de logiciels nécessaires sont les systèmes d'exploitation et de configuration.

Le système d'exploitation qui est utilisé dans pratiquement tous les équipements Cisco est la plate-forme logicielle Cisco IOS (Internetwork Operating System). Ce logiciel permet au matériel d'assurer sa fonction de routeur ou de commutateur. Le fichier de l'IOS occupe plusieurs méga-octets.

Le logiciel qu'utilise un routeur ou un commutateur est appelé fichier de configuration ou config. La configuration contient les instructions qui définissent comment l'équipement doit effectuer le routage ou la commutation. Un administrateur réseau crée une configuration qui définit la fonctionnalité souhaitée de l'équipement Cisco. La configuration peut spécifier des fonctions telles que l'adresse IP des interfaces, les protocoles de routage et les réseaux à annoncer. Le fichier de configuration occupe en général quelques centaines à quelques milliers d'octets.

Chaque composant logiciel est stocké en mémoire dans un fichier séparé. Ces fichiers sont également stockés dans différents types de mémoire. 1



L'IOS est stocké dans une zone de la mémoire appelée flash. La mémoire flash assure le stockage rémanent d'un IOS qui peut être utilisé comme système d'exploitation au démarrage. La mémoire permet la mise à niveau de l'IOS ou stocke plusieurs fichiers IOS. Dans de nombreuses architectures de routeur, l'IOS est copié et exécuté à partir de la mémoire vive (RAM).

Une copie du fichier de configuration est stockée en mémoire vive rémanente (NVRAM) pour être utilisée comme configuration au cours du démarrage. C'est ce que l'on appelle la « configuration de démarrage. La configuration de démarrage est copiée en RAM à l'amorçage. Cette configuration en RAM est celle utilisée pour faire fonctionner le routeur. C'est ce que l'on appelle la « configuration courante.

À compter de la version 12 de l'IOS, une interface unique vers tous les systèmes de fichiers qu'utilise un routeur est fournie. C'est ce que l'on appelle le système de fichiers IOS (IFS). L'IFS fournit une méthode unique pour la gestion de l'ensemble des systèmes de fichiers utilisés par un routeur. Il s'agit notamment des systèmes de fichiers de la mémoire flash, des systèmes de fichiers réseau (TFTP, RCP et FTP) et de lecture ou d'écriture de données (NVRAM, configuration courante, ROM). L'IFS utilise un jeu commun de préfixes pour spécifier les unités du système de fichiers. 2

Prefixe	Description
bootflash:	Mémoire bootflash
flash:	Mémoire flash. Ce préfixe est disponible sur toutes les plates-formes. Pour les plates-formes sans unité appelée flash, le préfixe flash: est associé à slot0:. Ainsi, le préfixe flash: peut être utilisé pour faire référence à la zone de mémoire flash principale sur toutes les plates-formes.
flh:	Fichiers journaux de chargement de la mémoire flash
ftp:	File Transfer Protocol (FTP) network server
nvram:	NVRAM
rcp:	Serveur de réseau RCP (Remote Copy Protocol)
Slot0:	Première carte mémoire flash PCMCIA (Personal Computer Memory Card International Association)
Slot1:	Deuxième carte mémoire flash PCMCIA
system:	Contient la mémoire système, y compris la configuration courante
Tftp:	Serveur de réseau TFTP

Il utilise la convention URL pour spécifier les fichiers sur les unités du réseau et sur le réseau. La convention URL identifie l'emplacement des fichiers de configuration à la suite du point-virgule sous la forme [[[//emplacement]/répertoire]/nomdefichier]. L'IFS prend également en charge le transfert de fichiers FTP.

Pre IOS Version 12.0 Commands	IOS Version 12.x Commands
configure network (pre-Cisco IOS Release 10.3) copy rcp running-config copy tftp running-config	copy ftp: system:running-config copy rcp: system:running-config copy tftp: system:running-config
configure overwrite-network (pre-Cisco IOS Release 10.3) copy rcp startup-config copy tftp startup-config	copy ftp: nvram:startup-config copy rcp: nvram:startup-config copy tftp: nvram:startup-config
show configuration (pre-Cisco IOS Release 10.3) show startup-config	more nvram:startup-config
write erase (pre-Cisco IOS Release 10.3) erase startup-config	erase nvram:
write memory (pre-Cisco IOS Release 10.3) copy running-config startup-config	copy system:running-config nvram:startup-config
write network (pre-Cisco IOS Release 10.3) copy running-config rcp copy running-config tftp	copy system:running-config ftp: copy system:running-config rcp: copy system:running-config tftp:
write terminal (pre-Cisco IOS Release 10.3) show running-config	more system:running-config

Activité de média interactive

Glisser-Positionner : Vue d'ensemble du système de fichiers IOS

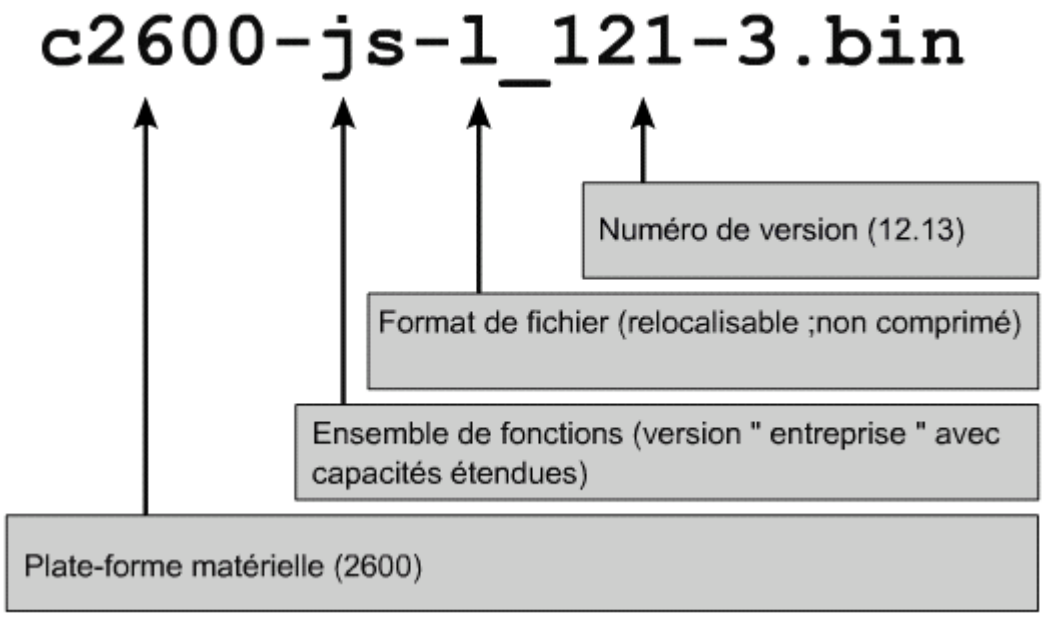
À la fin de cette activité, l'étudiant sera en mesure de citer les fichiers de configuration et leurs emplacements.

5.2 Gestion du système de fichiers Cisco

5.2.2 Conventions d'attribution de noms de l'IOS

Cisco développe plusieurs versions différentes de l'IOS. Ce systèmes prend en charge des plates-formes et des fonctions matérielles variées. Cisco développe et publie continuellement de nouvelles versions de l'IOS.

Pour identifier les différentes versions de son système, Cisco utilise une convention d'attribution de noms pour les fichiers IOS. Cette convention spécifie différents champs dans les noms. Ces champs contiennent notamment l'identification de la plate-forme matérielle, l'identification du jeu de fonctions et la version numérique. 1



La première partie du nom de fichier IOS identifie la plate-forme matérielle pour laquelle cette image est conçue.

La deuxième partie identifie les diverses fonctions incluses dans le fichier. De nombreuses fonctions sont proposées. Elles sont regroupées dans des images logicielles. Chaque fonction contient un sous-ensemble spécifique de fonctions IOS. Voici des exemples de catégories de jeux de fonction:

- **Basic** – Un jeu de fonctions de base pour la plate-forme matérielle, par exemple IP et IP/FW
- **Plus** – Un jeu de fonctions de base, plus des fonctions supplémentaires telles qu'IP Plus, IP/FW Plus et Enterprise Plus
- **Encryption** – L'ajout des jeux de fonctions de cryptage de données 56 bits, comme Plus 56, à un jeu de fonctions «basic» ou «plus». Il peut s'agir par exemple d'IP/ATM PLUS IPSEC 56 ou d'Enterprise Plus 56. À partir de la version 12.2 de la plate-forme logicielle Cisco IOS, les indicateurs de cryptage k8 et k9 sont utilisés:
- **k8** – Inférieur ou égal au cryptage sur 64 bits à partir de la version 12.2 de l'IOS
- **k9** – Supérieur au cryptage sur 64 bits (sur 12.2 et versions supérieures)

La troisième partie du nom indique le format de fichier. Elle indique si l'IOS est stocké en mémoire flash dans un fichier compressé et s'il est transférable. Si l'image flash est compressée, l'IOS doit être décompressé à l'amorçage lors de sa copie dans la mémoire RAM. Une image transférable est copiée de la mémoire flash dans la mémoire RAM pour y être exécutée. Une image non transférable est directement exécutée dans la mémoire flash.

La quatrième partie du nom de fichier identifie la version de l'IOS. Ce numéro de version numérique s'incrémente à mesure que Cisco développe de nouvelles versions de l'IOS.

Activité de média interactive

Glisser-Positionner : Conventions d'attribution de noms de l'IOS

À la fin de cette activité, l'étudiant sera en mesure d'identifier les différents champs du nom de l'image IOS.

5.2 Gestion du système de fichiers Cisco

5.2.3 Gestion des fichiers de configuration à l'aide de TFTP

Dans un routeur ou un commutateur Cisco, la configuration courante est en mémoire RAM et la configuration de démarrage est stockée par défaut dans la mémoire NVRAM. Pour prévenir une perte éventuelle de la configuration, cette configuration de démarrage doit être sauvegardée. L'une des copies de sauvegarde de la configuration peut être stockée sur un serveur TFTP. La commande **`copy running-config tftp`** peut être utilisée pour cela. 1 Les étapes de ce processus sont énumérées ci-après:

```
GAD#copy running-config tftp
Address or name of remote host
[]?192.168.119.20
Destination filename [GAD-confg]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
624 bytes copied in 7.05 secs
GAD#
```

- Entrez la commande **`copy running-config tftp`**.
- À l'invite, entrez l'adresse IP du serveur TFTP pour stocker le fichier de configuration.
- Entrez le nom que vous voulez attribuer au fichier de configuration ou acceptez le nom par défaut.
- Confirmez les choix en tapant yes chaque fois.

La configuration du routeur peut être restaurée en chargeant le fichier de sauvegarde de la configuration à partir d'un serveur TFTP. 2 Les étapes suivantes décrivent ce processus:

```
GAD#copy tftp running-config
Address or name of remote host []?
192.168.119.20
Source filename []?GAD-confg
Destination filename [running-config]?
Accessing tftp://192.168.119.20/GAD-
confg…
Loading GAD-confg from 192.168.119.20
(via FastEthernet 0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK-624 bytes]
624 bytes copied in 9.45 secs
GAD#
```

- Entrez la commande **`copy tftp running-config`**.
- À l'invite, sélectionnez un fichier de configuration d'hôte ou de réseau.
- À l'invite du système, tapez l'adresse IP du serveur TFTP où se trouve le fichier de configuration.
- À l'invite du système, entrez le nom du fichier de configuration ou acceptez le nom par défaut.
- Confirmez le nom du fichier de configuration et l'adresse du serveur fournis par le système.

Activité de TP

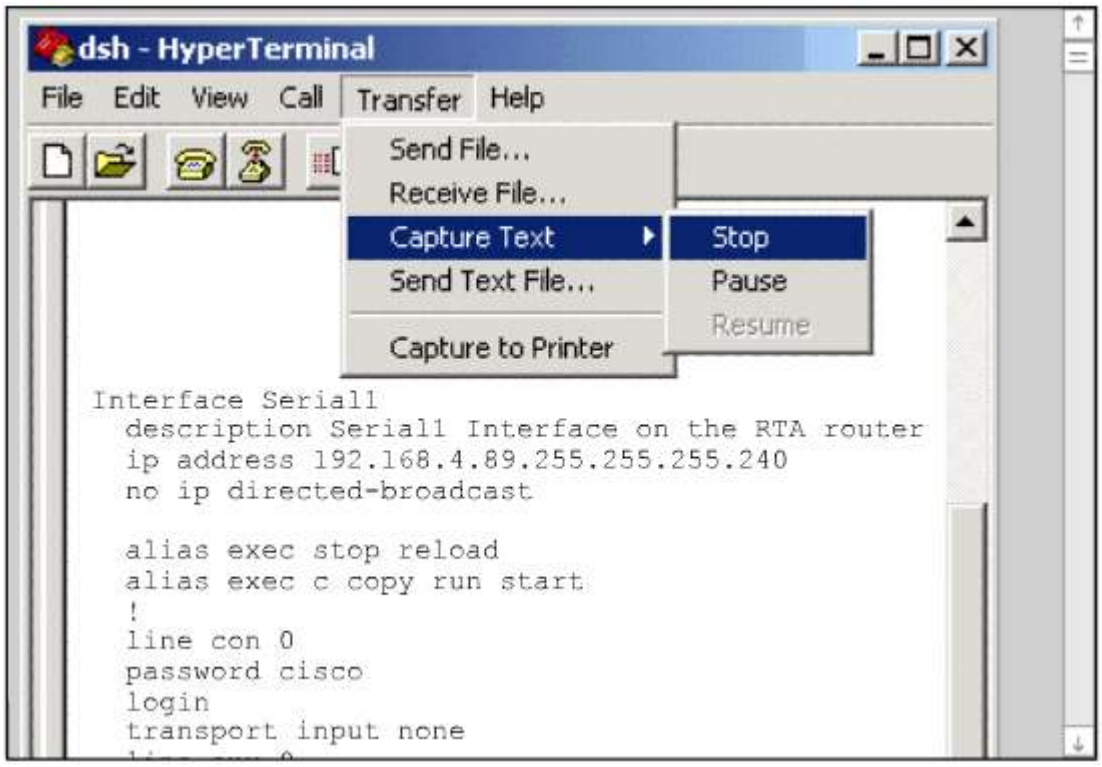
Exercice : Gestion des fichiers de configuration avec TFTP
Au cours de ce TP, les étudiants vont sauvegarder une copie du fichier de sauvegarde du routeur puis recharger le

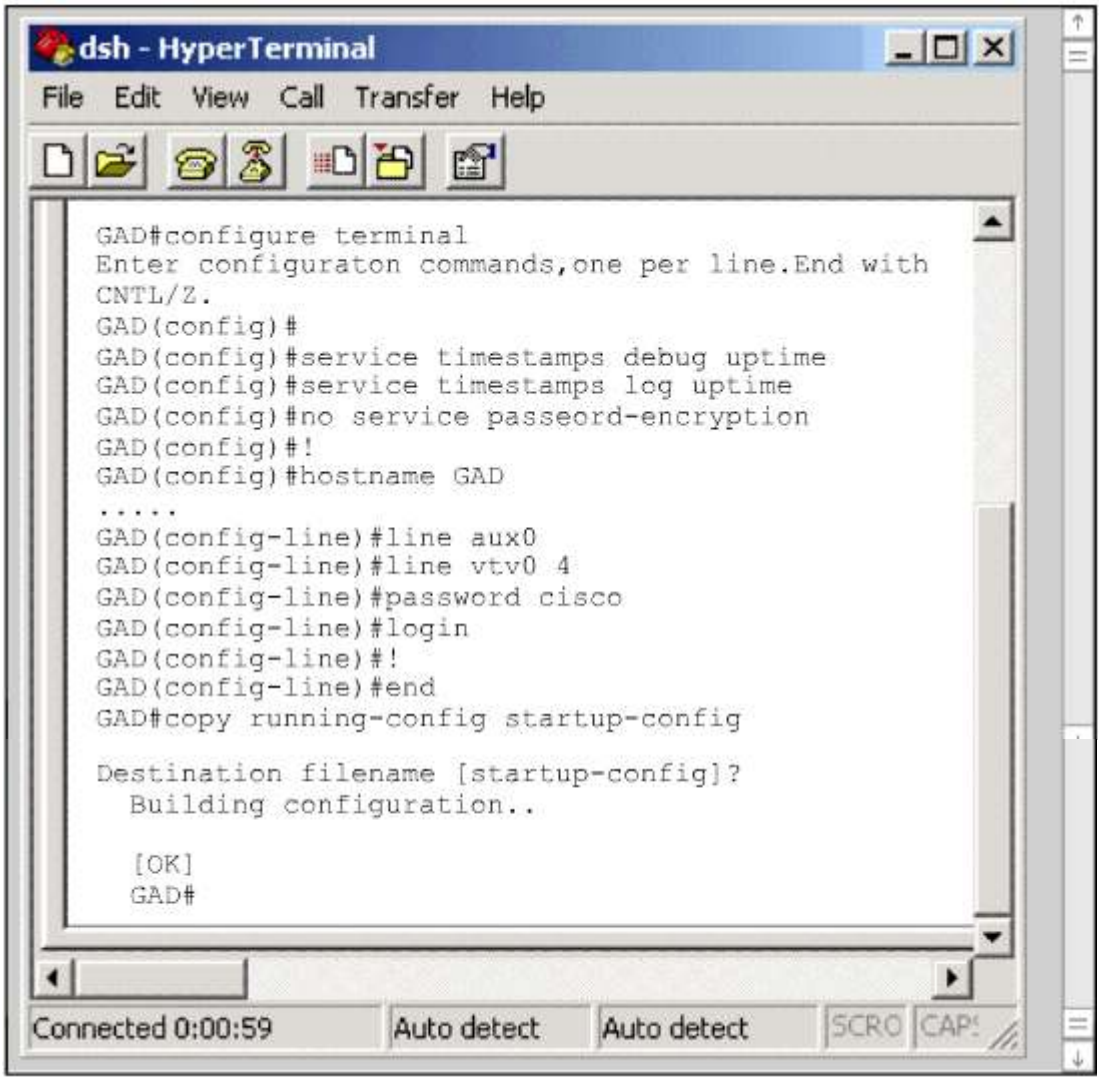
fichier de configuration de sauvegarde à partir d'un serveur TFTP dans la mémoire RAM d'un routeur.

5.2 Gestion du système de fichiers Cisco

5.2.4 Gestion des fichiers de configuration par copier-coller

Une autre façon de créer une copie de sauvegarde consiste à capturer les informations affichées par la commande **`show running-config`**. Cela est possible à partir d'une session de terminal. Il suffit de copier le résultat, de le copier dans un fichier texte, puis d'enregistrer le fichier texte. Quelques modifications devront ensuite être apportées au fichier avant de l'utiliser pour restaurer la configuration sur le routeur. 1 2





Pour capturer la configuration en utilisant le texte affiché sur l'écran HyperTerminal:

1. Sélectionnez **Transfert**
2. Sélectionnez **Capturer le texte**
3. Indiquez le nom du fichier texte pour la capture de la configuration
4. Sélectionnez **Démarrer** pour commencer la capture du texte
5. Affichez la configuration à l'écran en entrant **`show running-config`**
6. Appuyez sur la **barre d'espacement** chaque fois que l'invite **"- More –"** apparaît.

Lorsque la configuration complète est affichée, arrêtez la capture en procédant comme suit:

1. Sélectionnez **Transfert**
2. Sélectionnez **Capturer le texte**
3. Sélectionnez **Arrêter**

Une fois la capture terminée, vous devez modifier le fichier de configuration pour supprimer le texte superflu. Pour adapter ces informations afin de pouvoir les recoller dans le routeur, supprimez tout texte inutile de la configuration capturée. Vous pouvez ajouter des commentaires à la configuration afin d'en expliquer certaines parties. Il suffit pour cela de placer un point d'exclamation "!" en début de ligne.

Le fichier de configuration peut être modifié à l'aide d'un éditeur de texte tel que le Bloc-notes. Pour utiliser le Bloc-notes, cliquez sur **Fichier** > **Ouvrir**. Trouvez le fichier capturé et sélectionnez-le. Cliquez sur **Ouvrir**.

Vous devez supprimer les lignes qui contiennent:

- `show running-config`

- `Building configuration...`
- `Current configuration:`
- `- More -`
- `Ainsi que les lignes qui suivent le mot "End".`

À la fin de chaque section d'interface, ajoutez la commande **`no shutdown`**. Cliquez ensuite sur **Fichier** > **Enregistrer** pour enregistrer la version propre de la configuration.

La configuration de sauvegarde peut être restaurée à partir d'une session HyperTerminal. Avant de procéder à la restauration, vous devez supprimer du routeur toute trace de configuration. Pour ce faire, entrez la commande **`erase startup-config`** à l'invite privilégiée puis redémarrez le routeur en entrant la commande **`reload`**.

HyperTerminal peut également être utilisé pour restaurer une configuration. La sauvegarde propre de la configuration peut être copiée dans le routeur.

- Passez en mode de configuration globale du routeur.
- À partir d'HyperTerminal, cliquez sur **Transfert** > **Envoyer un fichier texte**.
- Sélectionnez le nom du fichier pour la configuration de sauvegarde enregistrée.
- Les lignes du fichier seront introduites dans le routeur comme si vous les tapiez.
- Recherchez toute erreur éventuelle.
- Une fois la configuration entrée, appuyez sur la touche **Ctrl-Z** pour quitter le mode de configuration globale.
- Restaurez la configuration de démarrage à l'aide de **`copy running-config startup-config`**.

5.2 Gestion du système de fichiers Cisco

5.2.5 Gestion des images IOS via TFTP

De temps à autre, vous devez mettre à jour au restaurer l'IOS. Dès que vous recevez un routeur, il est conseillé de sauvegarder son système d'exploitation. Cette image IOS peut être stockée dans un serveur central avec d'autres images IOS. Ces images peuvent être utilisées pour restaurer ou mettre à niveau l'IOS sur les routeurs et commutateurs de l'interréseau.

Un service TFTP doit s'exécuter sur ce serveur. La sauvegarde de l'IOS peut être démarrée à partir du mode privilégié l'aide de la commande **`copy flash tftp`**. Le routeur demandera à l'utilisateur d'entrer l'adresse IP du serveur TFTP ainsi que spécifier un nom pour le fichier de destination.

L'IOS peut être restauré ou mis à jour avec l'aide de la commande **`copy tftp flash`**. Le routeur demandera de nouveau à l'utilisateur d'entrer l'adresse IP du serveur TFTP. Lorsque l'utilisateur indique le nom de fichier de l'image IOS sur le serveur, le routeur lui demande ensuite s'il souhaite effacer la mémoire flash. C'est souvent le cas lorsqu'il n'y a pas suffisamment de mémoire flash disponible pour la nouvelle image. Lors de l'effacement de l'image de la mémoire flash, une série de « e » apparaît pour montrer la progression du processus. 1

```
GAD#copy tftp flash
Address or name of remote host []?192.168.119.20
Source filename []? C2600-js-l_121-3.bin
Destination filename [C2600-js-l_121-3.bin]?
Accessing tftp://192.168.119.20/ C2600-js-l_121-3.bin
Erase flash: before copying? [confirm]
Erasing the flash file system will remove all files
Continue? [confirm]
Erasing device eeeeee…eeeeeeeeeeeee…erased
Loading C2600-js-l_121-3.bin from 192.168.119.20 (via
FastEthernet 0/0): !!!!!!!!!!!!!!…!!!!!!!!!!!!!!!!!!
Verifying Check sum ............OK
[OK-8906589 bytes]
8906589 bytes copied in 277.45 secs
GAD#
```

Un (!) s'affiche chaque fois qu'un datagramme est téléchargé. Ce processus peut être long, étant donné que l'image IOS occupe plusieurs méga-octets.

La nouvelle image flash est vérifiée dès la fin de son téléchargement. Le routeur peut être alors rechargé pour utiliser la nouvelle image IOS.

Activité de TP

Exercice : Gestion des images IOS via TFTP

Au cours de ce TP, les étudiants vont sauvegarder une copie de l'IOS d'un routeur de la mémoire flash vers un serveur TFTP.

5.2 Gestion du système de fichiers Cisco

5.2.6 Gestion des images IOS via Xmodem

Si l'image IOS en mémoire flash a été effacée ou altérée, il peut être nécessire de restaurer l'IOS à partir du mode moniteur ROM (ROMmon). Dans plusieurs architectures matérielles Cisco, le mode ROMmon est identifié par l'invite rommon 1 >.

La première étape de ce processus consiste à déterminer pourquoi l'image IOS ne s'est pas chargée depuis la mémoire flash. Cela peut être dû à une image corrompue ou manquante. La mémoire flash doit être examinée avec la commande **dir flash:**.

Si vous détectez une image qui semble être valide, tentez de démarrer à partir de cette image. Utilisez la commande **boot flash:**. Par exemple, si le nom de l'image était c2600-is-mz.121-5, vous entrerez la commande:

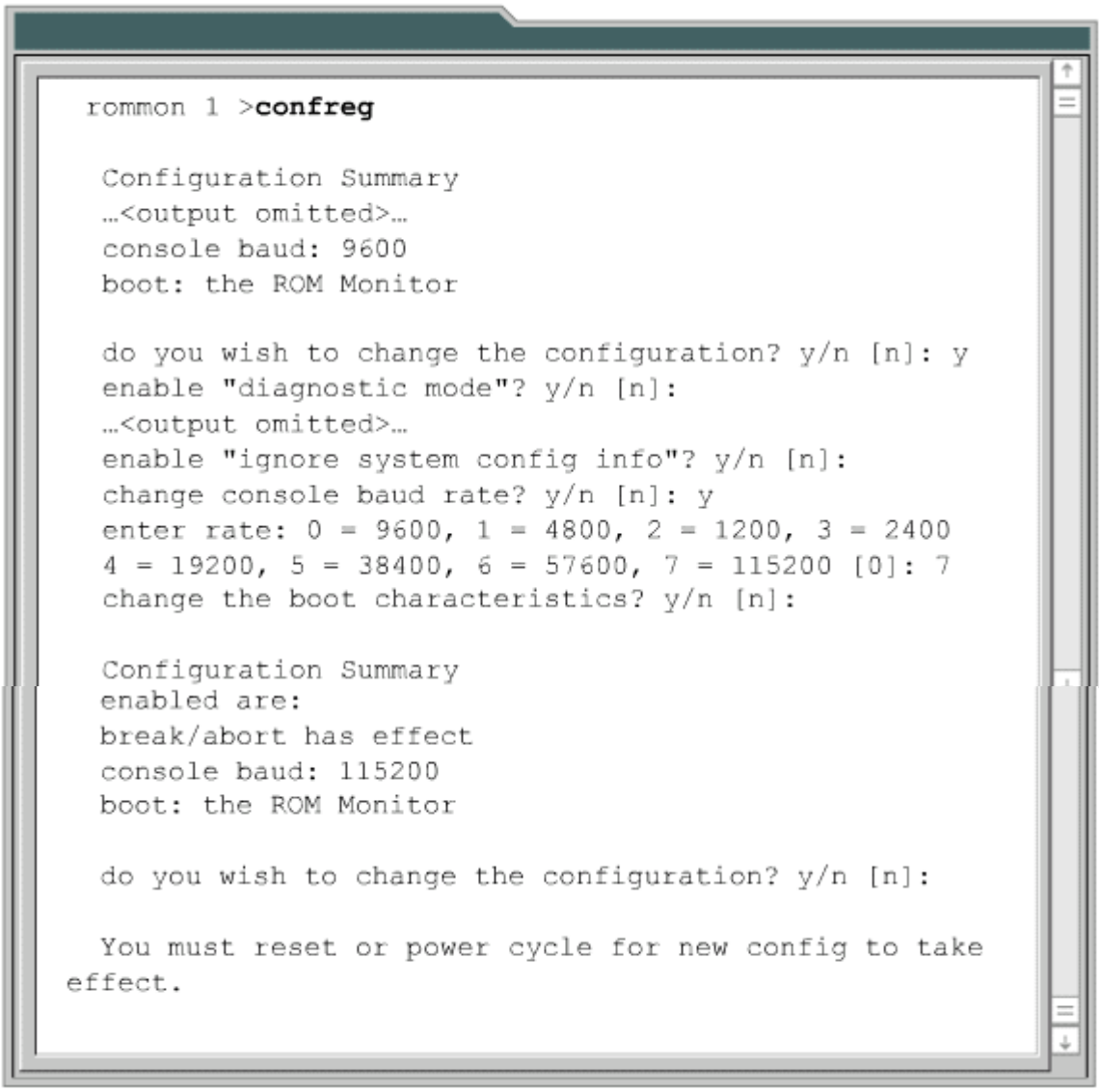
```
rommon 1>boot flash:c2600-is-mz.121-5
```

Si le routeur s'amorce correctement, vous devez examiner plusieurs éléments pour déterminer pourquoi le routeur s'est amorcé à partir de ROMmon plutôt que d'utiliser l'IOS de la mémoire flash. D'abord, utilisez la commande **show version** pour vérifier dans le registre de configuration s'il est configuré pour la séquence d'amorçage par défaut. Si la valeur du registre de configuration est correcte, utilisez la commande **show startup-config** pour rechercher une commande boot system ordonnant au routeur d'utiliser l'IOS pour ROM monitor.

Si le routeur ne s'amorce pas correctement à partir de l'image ou s'il n'y pas d'image IOS, vous devrez télécharger un nouvel IOS. Le fichier IOS peut être configuré soit en utilisant Xmodem pour restaurer l'image via la console, soit en téléchargeant l'image en utilisant TFTP à partir du mode ROMmon.

Télécharger en utilisant Xmodem à partir de ROMmon

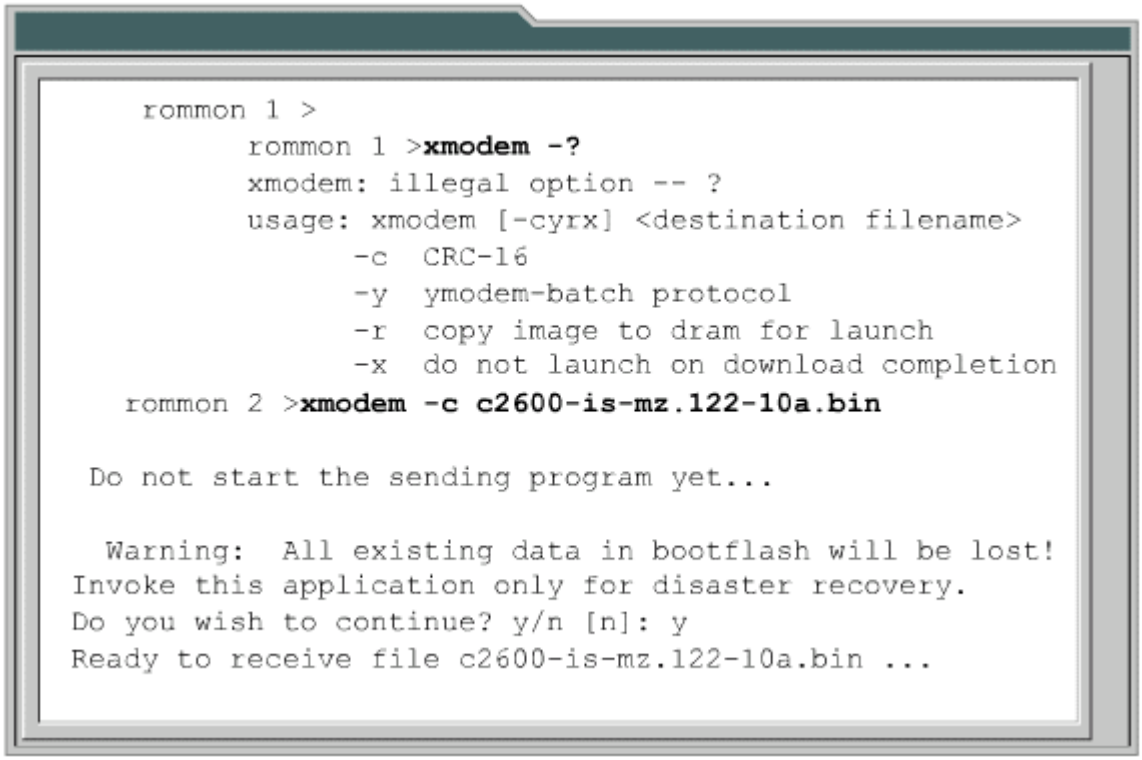
Pour que vous puissiez restaurer l'IOS via la console, le PC local doit contenir une copie du fichier IOS à restaurer et un programme d'émulation de terminal tel qu'HyperTerminal. L'IOS peut être restauré en utilisant la vitesse par défaut de 9600 bps de la console. Le débit peut être porté à 115200 bps pour accélérer le téléchargement. La vitesse de la console peut être changée à partir de ROMmon en utilisant la commande **confreg**. Après l'exécution de la commande **confreg**, le routeur demandera les divers paramètres qui peuvent être modifiés. 1



Lorsqu'il vous est demandé "change console baud rate? y/n [n]:" et que vous répondez **y**, une invite s'affiche pour sélectionner la vitesse. Après avoir modifié la vitesse de la console et redémarré le routeur en mode ROMmon, vous devez arrêter la session de terminal à 9600 bps et en démarrer une nouvelle à 115200 bps, vitesse identique à celle de la console.

Vous pouvez utiliser la commande Xmodem à partir du mode ROMmon pour restaurer l'image de l'IOS à partir du PC. Le format de la commande est **xmodem -c *cimage_file_name***. Par exemple, pour restaurer un fichier d'image IOS dont le nom est c2600-is-mz.122-10a.bin, tapez la commande:

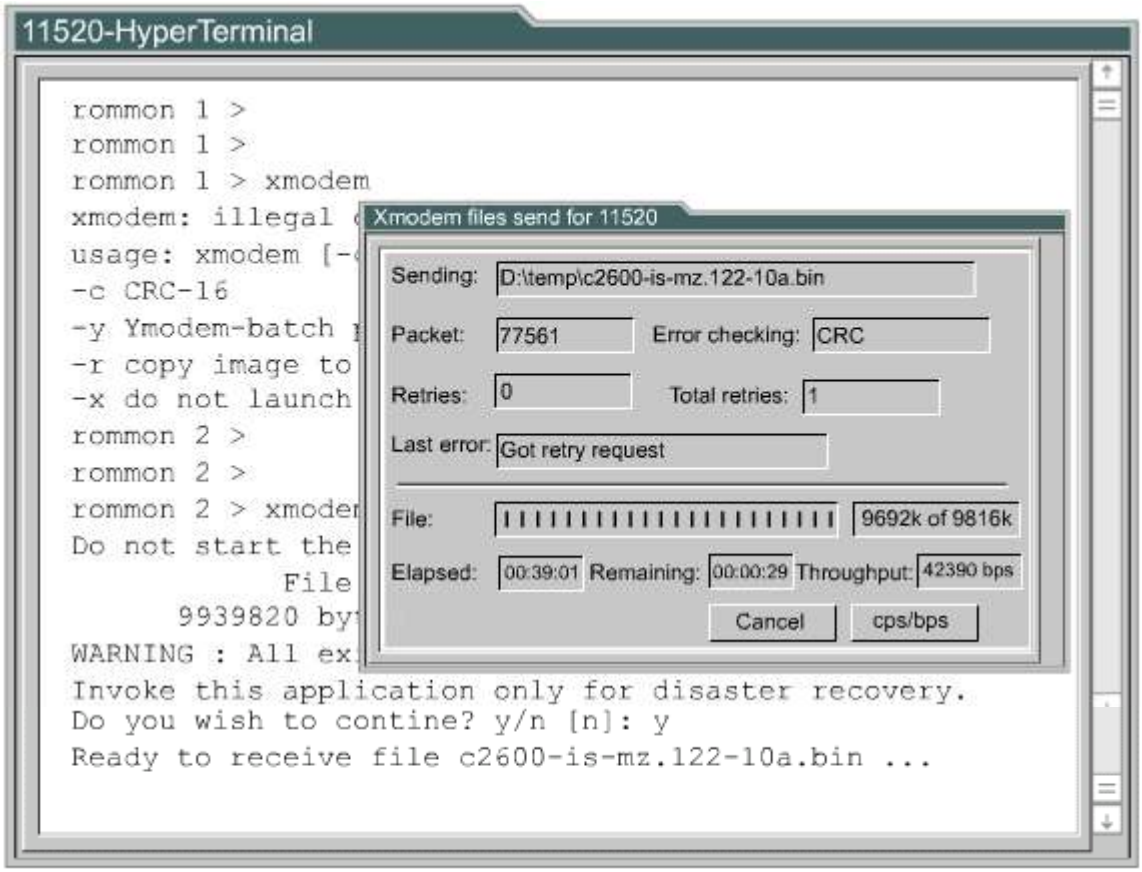
xmodem -c c2600-is-mz.122-10a.bin 2



Le **-c** indique au processus Xmodem d'utiliser le code de redondance cyclique (CRC) pour contrôler les erreurs au moment du téléchargement.

Le routeur vous demandera de ne pas commencer le transfert et affichera un message d'avertissement. Ce message indique que le bootflash va être effacé et vous demande si vous voulez poursuivre. Si vous continuez le processus, le routeur demande alors s'il peut lancer le transfert.

Vous devez alors lancer le transfert à partir de l'émulateur de terminal. Dans HyperTerminal, sélectionnez **Transfert** > **Envoyer un fichier**. Ensuite, dans la boîte de dialogue **Envoyer un fichier**, indiquez le nom/emplacement de l'image, sélectionnez Xmodem comme protocole, puis lancez le transfert. L'état du transfert apparaît dans la boîte de dialogue Envoi des fichiers. 3



Une fois le transfert terminé, un message apparaît, indiquant que la mémoire flash a été effacée. Le message Téléchargement terminé ! s'affiche ensuite. Avant de redémarrer le routeur, vous devez à nouveau paramétrer la vitesse à 9600 bps et le registre de configuration à 0x2102. Entrez la commande **`config-register 0x2102`** à l'invite du mode privilégié.

Lorsque le routeur se réamorce, vous devez arrêter la session de terminal à 115200 bps et démarrer celle à 9600 bps.

Activité de TP

Exercice : Procédures de récupération des mots de passe

Au cours de ce TP, les étudiants vont accéder à un routeur avec un mot de passe (enable) de mode privilégié inconnu.

Activité de TP

Exercice : Gestion des images IOS avec ROMmon et Xmodem

Au cours de ce TP, les étudiants vont récupérer un routeur de la gamme Cisco 1700 utilisant le moniteur ROM (ROMmon) (rommon >) en raison d'une image IOS d'amorçage manquante ou corrompue.

5.2 Gestion du système de fichiers Cisco

5.2.7 Variables d'environnement

L'IOS peut être restauré à partir d'une session TFTP. Le téléchargement en utilisant TFTP à partir de ROMmon est le moyen le plus rapide de restaurer une image de l'IOS sur le routeur. Vous devez pour cela définir des variables d'environnement, puis utiliser la commande **`tftpdnld`**.

Étant donné que ROMmon a des fonctions très limitées, aucun fichier de configuration n'est chargé durant l'amorçage. Le routeur n'a par conséquent aucune configuration d'IP ou d'interface. Les variables d'environnement fournissent une configuration minimale qui permettent transfert via TFTP de l'IOS. Le transfert ROMmon TFTP ne fonctionne que sur le premier port LAN, c'est pourquoi un jeu simple de paramètres IP a été défini pour cette interface. Pour définir une variable d'environnement ROMmon, vous devez taper le nom de la variable, le signe égal (=), puis la valeur de la variable

(VARIABLE_NAME=value). Par exemple, pour définir l'adresse IP à 10.0.0.1, tapez IP_ADDRESS=10.0.0.1 à l'invite ROMmon. 1

REMARQUE:
Tous les noms de variables tiennent compte des majuscules.

Les variables minimales nécessaires pour utiliser tftpdnld sont les suivantes:

- **IP_ADDRESS** – L'adresse IP sur l'interface LAN
- **IP_SUBNET_MASK** – Le masque de sous-réseau pour l'interface LAN
- **DEFAULT_GATEWAY** – La passerelle par défaut pour l'interface LAN
- **TFTP_SERVER** – L'adresse IP du serveur TFTP
- **TFTP_FILE** – Le nom du fichier IOS sur le serveur

Pour vérifier les variables d'environnement ROMmon, la commande **`set`** peut être utilisée. 1

```
rommon 10>set
 IP_ADDRESS=10.0.0.1
 IP_SUBNET_MASK=255.255.255.0
 DEFAULT_GATEWAY=10.0.0.254
 TFTP_SERVER=192.168.1.1
 TFTP_FILE=GAD/original_2003_Jan_22/c2600-i-mz.121-5
```

Une fois que les variables sont définies pour le téléchargement de l'IOS, la commande **`tftpdnld`** est entrée sans arguments. Le ROMmon propage alors les variables et un message de confirmation apparaît, indiquant que la mémoire flash sera effacée. 2

```
rommon 12 >tftpdnld
              IP_ADDRESS: 10.0.0.1
          IP_SUBNET_MASK: 255.255.255.0
         DEFAULT_GATEWAY: 10.0.0.254
             TFTP_SERVER: 192.168.1.1
               TFTP_FILE: GAD/original_2003_Jan_22/
                          c2600-i-mz.121-5
         Invoke this command for disaster recovery only.
         WARNING: all existing data in all partitions on
                  flash will be lost!
         Do you wish to continue? y/n:  [n]:  y
         Receiving GAD/original_2003_Jan_22/c2600-i-
mz.121-5 from 192.168.1.1!!!!.!!!!!!!!!!!!!!!!!!.!!
         File reception completed.
         Copying file GAD/original_2003_Jan_22/c2600-i-
mz.121-5 to flash.
         Erasing flash at 0x607c0000
         program flash location 0x60440000
         rommon 13>
```

Un ! s'affiche à chaque réception d'un datagramme du fichier de l'IOS. Une fois la réception terminée, la mémoire flash est effacée et le nouveau fichier d'image de l'IOS est écrit. Plusieurs messages s'affichent au terme du processus.

Après l'écriture de la nouvelle image en mémoire flash et lorsque l'invite ROMmon s'affiche, le routeur peut être redémarré en tapant **i**. Il doit à présent s'amorcer à partir de la nouvelle image IOS en mémoire flash.

5.2 Gestion du système de fichiers Cisco

5.2.8 Vérification du système de fichiers

Plusieurs commandes vous permettent de vérifier le système de fichiers du routeur. La commande **show version** est l'une d'elles. 1 La commande **show version** peut être utilisée pour vérifier l'image actuelle et la quantité totale de mémoire flash. Elle vérifie également deux autres éléments concernant le chargement de l'IOS. Elle identifie l'origine de l'image IOS que le routeur a utilisée pour l'amorçage et affiche le registre de configuration. Le paramètre du champ d'amorçage du registre de configuration peut être examiné pour déterminer à partir d'où le routeur va charger l'IOS. Si ces valeurs ne correspondent pas, cela peut provenir d'une image IOS corrompue ou manquante en mémoire flash ou de la présence de commandes boot system dans la configuration de démarrage.

```
BHM#show version
Cisco Internetwork Operating System Software
IOS (tm) 1700 Software (C1700-BNSY-L), Version
12.2(11)P, RELEASE SOFTWARE (fc1)
… <output omitted>…
System image file is "flash:c1700-bnsy-1.122-
11.p", booted via flash
cisco 171 (68360) processor (revision C) with
3584K/512K bytes of memory.
Processor board ID 12014633, with hardware
revision 00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP
compliant.
1 Ethernet/IEEE 802.3 interface(s)
2  serial(sync/async) network interface(s)
System/IO memory with parity disabled
2048K bytes of DRAM onboard 2048K bytes of DRAM on
SIMM
System running from FLASH
8K bytes of non-volatile configuration memory.
6144K bytes of processor board PCMCIA flash (Read
ONLY)
Configuration register is 0x2102
BHM#
```

La commande **show flash** peut également être utilisée pour vérifier le système de fichiers. 2 Cette commande sert à identifier la ou les image(s) IOS en mémoire flash ainsi que la quantité de mémoire flash disponible. Elle est souvent utilisée pour confirmer qu'il y a amplement assez d'espace pour stocker une nouvelle image IOS.

```
BHM#show flash
PCMCIA flash directory:
File  Length    Name/status
  1   6007232   c1700-bnsy-1.212-11.p
[6007296 bytes used, 284160 available, 6291456
total]
6144K bytes of processor board PCMCIA flash (Read
ONLY)
BHM#
```

Résumé

Comme nous l'avons déjà indiqué, le fichier de configuration peut contenir des commandes boot system. Ces dernières peuvent être utilisées pour identifier l'origine de l'image d'amorçage IOS souhaitée. Plusieurs commandes boot system peuvent être utilisées pour créer une séquence de secours pour découvrir et charger un IOS. Ces commandes boot system seront traitées dans l'ordre de leur apparition dans le fichier de configuration.

- **Résumé**Identifier les étapes de la séquence d'amorçage d'un routeur
- Déterminer comment un équipement Cisco localise et charge l'IOS
- Utiliser la commande **`boot system`**
- Identifier les valeurs du registre de configuration
- Résoudre les problèmes
- Identifier les fichiers utilisés par l'IOS et leurs fonctions
- Identifier les emplacements des différents types de fichiers sur le routeur
- Identifier les différentes parties du nom IOS
- Gérer des fichiers de configuration à l'aide de TFTP
- Gérer des fichiers de configuration par copier-coller
- Gérer des images IOS via TFTP
- Gérer des images IOS via XModem
- Vérifier le système de fichiers à l'aide des commandes **`show`**

Résumé

- Les routines de démarrage du routeur sont les suivantes :
  - Tester les composants matériels du routeur
  - Rechercher et charger la plate-forme logicielle Cisco IOS
  - Rechercher et appliquer les instructions de configuration
- La plate-forme logicielle Cisco IOS est stockée dans la mémoire flash.
- Le fichier de configuration est stocké dans la mémoire NVRAM pour être utilisé lors du démarrage.

Vue d'ensemble

Le routage n'est rien d'autre que la spécification de directions pour naviguer de réseau en réseau. Ces directions, également appelées routes, peuvent être indiquées de façon dynamique par un autre routeur ou attribuées de façon statique par un administrateur.

Ce module introduit le concept de protocoles de routage dynamique. Il décrit les classes du protocole de routage dynamique et donne des exemples de protocoles dans chacune de ces classes.

Un administrateur réseau choisit un protocole de routage dynamique en fonction de nombreuses considérations. La taille du réseau, la bande passante des liaisons disponibles, la puissance de traitement des routeurs du réseau, les marques et les modèles de routeurs sur le réseau ainsi que les protocoles déjà utilisés sont autant de facteurs à prendre en compte. Ce module détaille les différences entre des protocoles de routage afin d'aider les administrateurs réseau à faire leur choix.

À la fin de ce module, les étudiants doivent être en mesure de:

- Expliquer la signification du routage statique
- Configurer les routes statiques et les routes par défaut
- Vérifier et dépanner les routes statiques et les routes par défaut
- Identifier les classes de protocoles de routage
- Identifier les protocoles de routage à vecteur de distance
- Identifier les protocoles de routage à état de liens
- Décrire les caractéristiques de base des protocoles de routage communs
- Identifier les protocoles IGP
- Identifier les protocoles EGP
- Activer le protocole RIP (Routing Information Protocol) sur un routeur

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
6.1	Introduction au routage statique
6.2	Vue d'ensemble du routage dynamique
6.3	Vue d'ensemble des protocoles de routage

Ce module porte sur les objectifs suivants de l'examen de certificationCCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Sélection d'un protocole de routage approprié d'après les besoins des utilisateurs	• Configuration de protocoles de routage d'après les besoins des utilisateurs • Mise en œuvre d'un LAN		• Évaluation des caractéristiques des protocoles de routage

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Sélection d'un protocole de routage approprié d'après les besoins des utilisateurs • Conception ou modification d'un LAN simple à l'aide de produits Cisco	• Configuration de protocoles de routage d'après les besoins des utilisateurs • Mise en œuvre d'un LAN		• Évaluation des caractéristiques des protocoles de routage

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
• Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	• Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	• Description des concepts associés au routage, ainsi que des différents protocoles et méthodes visant à sa réalisation

6.1 Introduction au routage statique

6.1.1 Présentation du routage

Le routage est le processus qu'un routeur utilise pour transmettre des paquets vers un réseau de destination. Un routeur prend des décisions en fonction de l'adresse IP de destination d'un paquet. Tout le long du chemin, les divers équipements se servent de l'adresse IP de destination pour orienter le paquet dans la bonne direction afin qu'il arrive à destination. Pour prendre les bonnes décisions, les routeurs doivent connaître la direction à prendre jusqu'aux réseaux distants. Lorsque les routeurs utilisent le routage dynamique, ces informations sont fournies par les autres routeurs. Lorsque le routage statique est utilisé, un administrateur réseau configure manuellement les informations sur les réseaux distants.

Étant donné que les routes statiques doivent être configurées manuellement, toute modification de la topologie réseau oblige l'administrateur à ajouter et supprimer des routes statiques pour tenir compte des modifications. Dans un grand réseau, cette maintenance manuelle des tables de routage peut générer une forte charge de travail administratif. Sur les petits réseaux où peu de modifications sont possibles, les routes statiques ne requièrent que très peu de maintenance. En raison des impératifs administratifs, le routage statique n'offre pas la même évolutivité que le routage dynamique. Même dans les grands réseaux, les routes statiques qui sont prévues pour atteindre un but précis sont souvent configurées en conjonction avec un protocole de routage dynamique.

Statique

Utilise une route programmée dans le routeur par un administrateur réseau.

Dynamique

Utilise une route qu'un protocole de routage modifie automatiquement en fonction des changements de topologie ou de trafic.

6.1 Introduction au routage statique

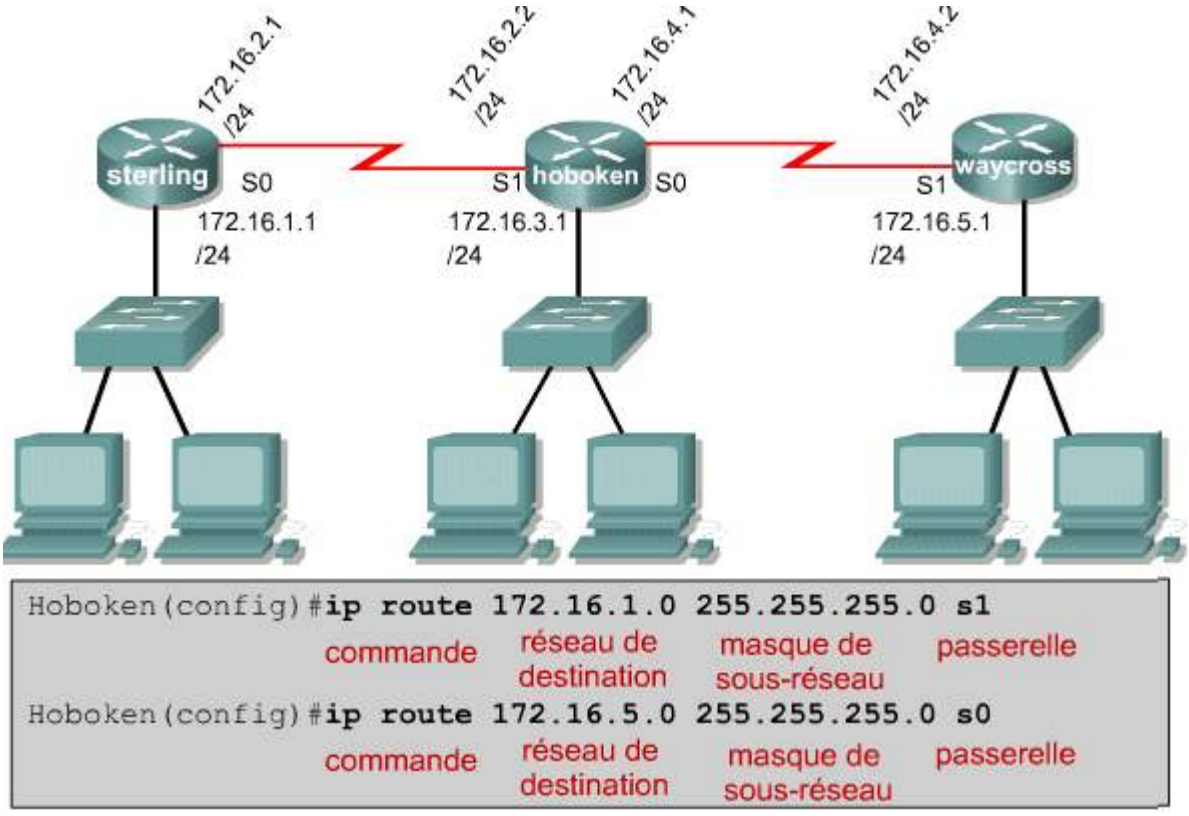
6.1.2 Utilisation de la route statique

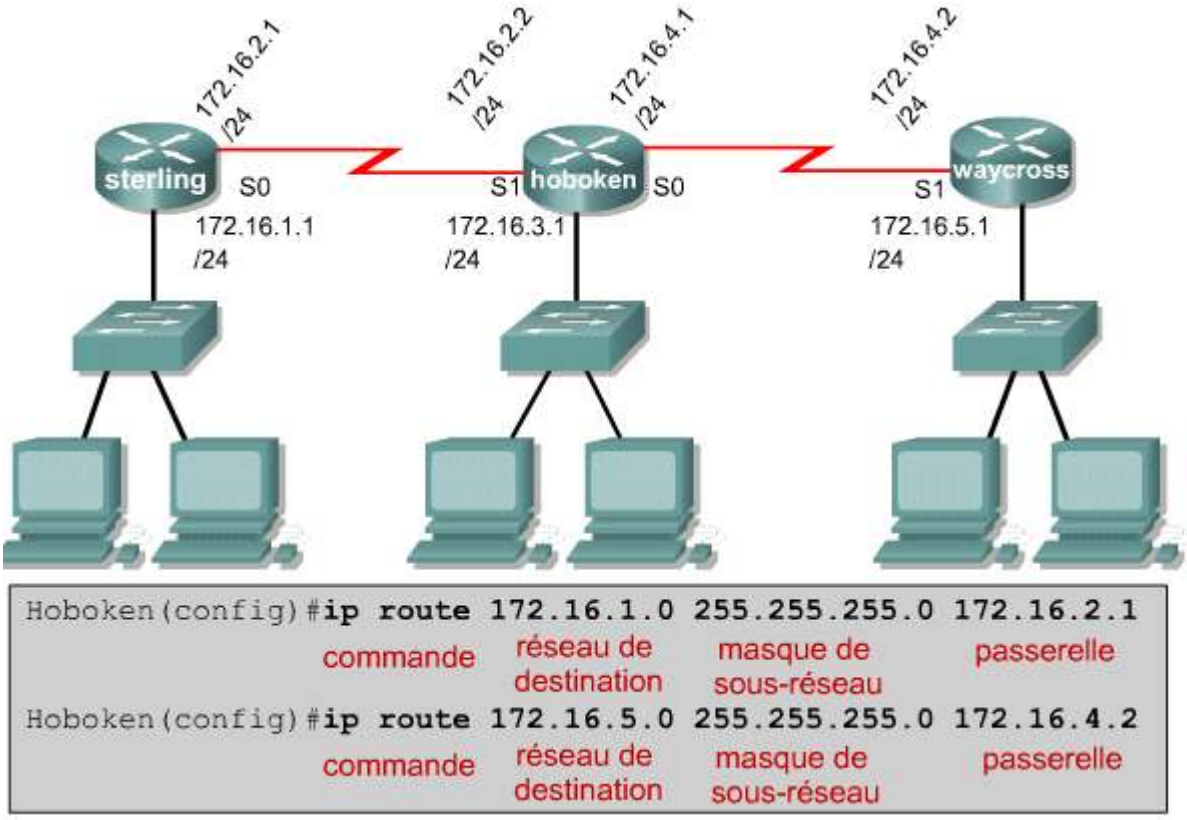
Les opérations de routage statique s'articulent en trois parties:

- L'administrateur réseau configure la route
- Le routeur insère la route dans la table de routage
- Les paquets sont acheminés à l'aide de la route statique

Puisqu'une route statique est configurée manuellement, l'administrateur doit la configurer sur le routeur à l'aide de la commande **`ip route`**. La syntaxe correcte de la commande **`ip route`** est illustrée à la figure 1

Dans les figures 2 et 3, l'administrateur réseau du routeur Hoboken doit configurer une route statique qui pointe sur les réseaux 172.16.1.0/24 et 172.16.5.0/24 liés aux autres routeurs. L'administrateur peut entrer l'une ou l'autre des deux commandes pour atteindre cet objectif. La méthode de la figure 2 spécifie l'interface sortante. La méthode de la figure 3 spécifie l'adresse IP du saut suivant du routeur adjacent. L'une ou l'autre des commandes insèrera une route statique dans la table de routage du routeur Hoboken.





La distance administrative est un paramètre optionnel qui donne une mesure de la fiabilité de la route. Plus la valeur de la distance administrative est faible et plus la route est fiable. Ainsi, une route dont la distance administrative est faible sera insérée avant une route identique dont la distance administrative est élevée. La distance administrative par défaut est 1 quand on utilise une route statique. Lorsqu'une interface de sortie est configurée comme passerelle dans une route statique, la route statique apparaît comme étant directement connectée. Ceci peut parfois porter à confusion, car une route vraiment directement connectée a une distance administrative de 0. Pour vérifier la distance administrative d'une route donnée. Utilisez la commande **show ip route** *adresse*, où l'option adresse est l'adresse IP de cette route. Si l'on souhaite une distance administrative autre que celle par défaut, il faut entrer une valeur comprise entre 0 et 255 après le saut suivant ou l'interface sortante:

```
waycross(config)#ip route 172.16.3.0 255.255.255.0 172.16.4.1 130
```

Si le routeur ne peut pas atteindre l'interface sortante qui est empruntée sur la route, la route n'est pas installée dans la table de routage. Cela veut dire que si cette interface est arrêtée, la route n'est pas inséré dans la table de routage.

Les routes statiques sont quelques fois utilisées à des fins de sauvegarde. Il est possible de configurer sur un routeur une route statique qui ne sera utilisée qu'en cas d'échec de la route acquise de façon dynamique. Pour utiliser une route statique de cette manière, attribuez simplement une valeur de distance administrative supérieure à celle du protocole de routage dynamique utilisé.

Activité de TP

Activité en ligne : Utilisation de la route dynamique

Au cours de ce TP, l'étudiant va apprendre à créer une route statique.

Activité de TP

Activité en ligne : Routes statiques

Au cours de ce TP, les étudiants vont s'entraîner à utiliser des routes statiques en dépannant un réseau connecté de la façon décrite sur la carte topologique.

6.1 Introduction au routage statique

6.1.3 Configuration de routes statiques

Cette section décrit les étapes de configuration des routes statiques et donne un exemple de réseau simple pour lequel des routes statiques peuvent être configurées.

Pour configurer des routes statiques, procédez comme suit:

Étape 1: Déterminez tous les préfixes, masques et adresses désirés. Les adresses peuvent être soit une adresse locale, soit une adresse de saut suivant qui mène à l'adresse désirée.

Étape 2: Passez en mode de configuration globale.

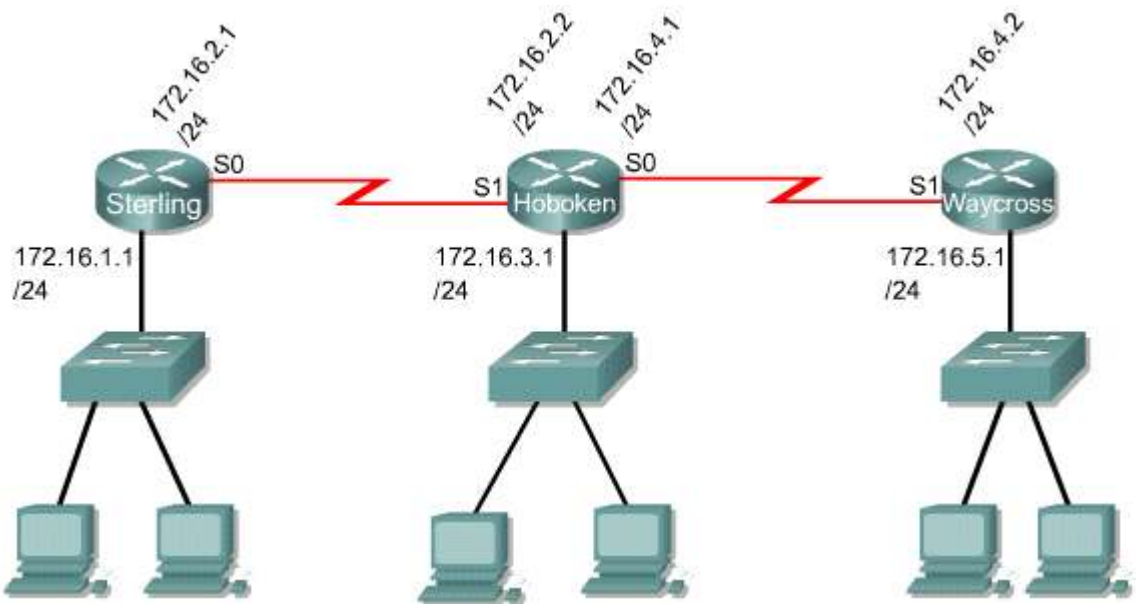
Étape 3: Tapez la commande **`ip route`** avec une adresse de destination et un masque de sous-réseau, suivis de la passerelle correspondante de l'étape 1. L'inclusion d'une distance administrative est facultative.

Étape 4: Répétez l'étape 3 pour autant de réseaux de destination que définis à l'étape 1.

Étape 5: Quittez le mode de configuration globale.

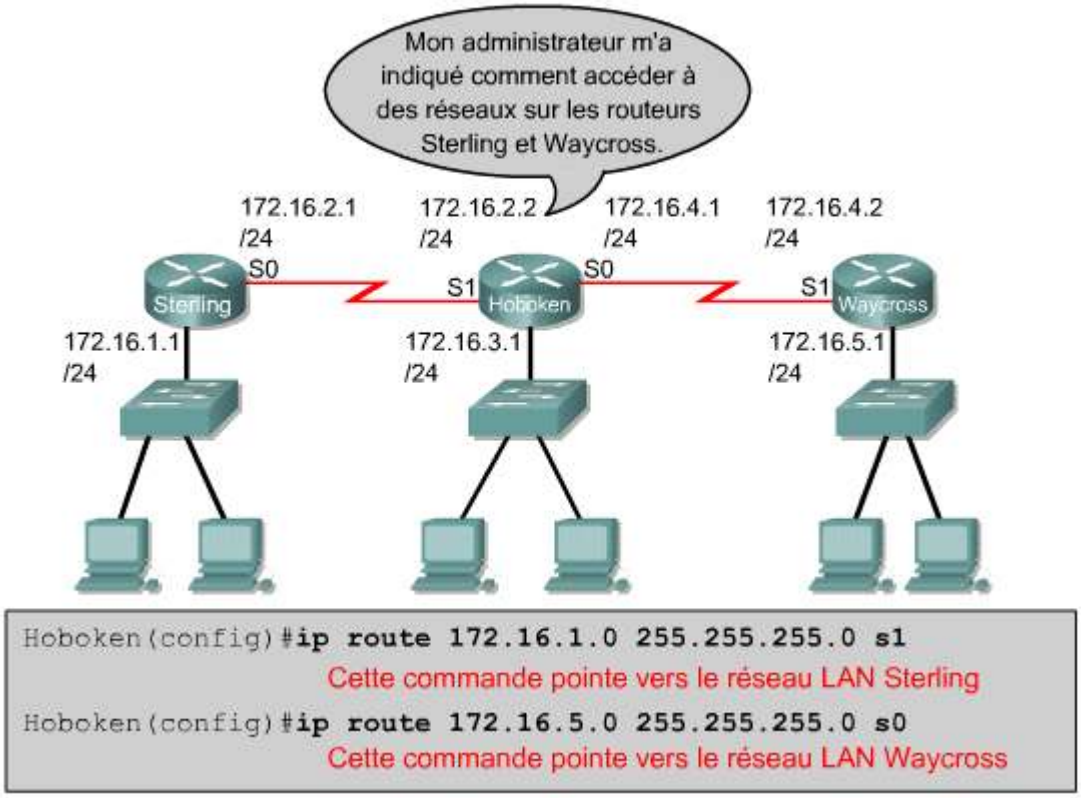
Étape 6: Enregistrez la configuration courante en mémoire NVRAM en utilisant la commande **`copy running-config startup-config`**.

Le réseau de l'exemple est une configuration simple comportant trois routeurs. 1Hoboken doit être configuré de façon à pouvoir atteindre le réseau 172.16.1.0 et le réseau 172.16.5.0. Ces deux réseaux possèdent un masque de sous-réseau 255.255.255.0.



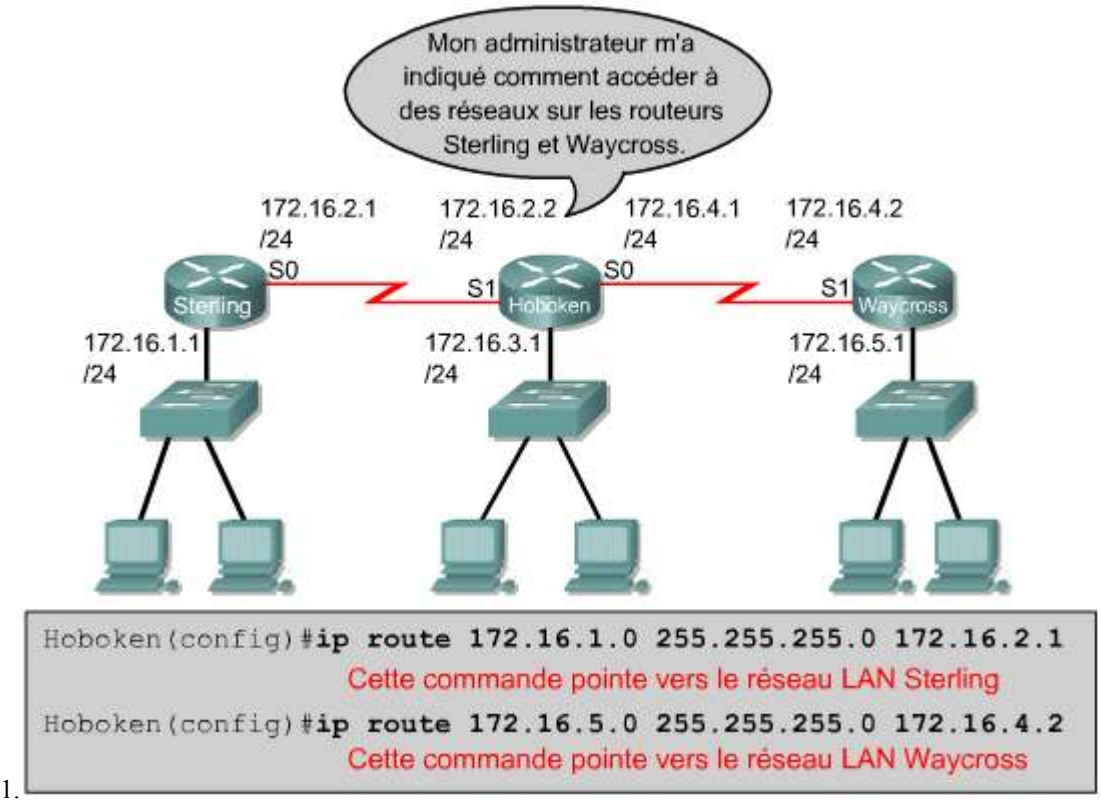
Les paquets dont le réseau de destination est 172.16.1.0 doivent être acheminés vers Sterling et ceux dont l'adresse de destination est 172.16.5.0 doivent être routés vers Waycross. Vous pouvez configurer des routes statiques pour accomplir cette tâche.

Les deux routes statiques seront d'abord configurées pour utiliser une interface locale comme passerelle vers les réseaux de destination. 2Comme l'adresse administrative n'a pas été spécifiée, elle prendra la valeur 1 par défaut quand la route est installée dans la table de routage.



Les deux mêmes routes statiques peuvent également être configurées à l'aide d'une adresse du saut suivant comme passerelle. 3 La première route vers le réseau 172.16.1.0 possède une passerelle 172.16.2.1. La deuxième route vers le réseau 172.16.5.0 a une passerelle 172.16.4.2. Puisque la distance administrative n'a pas été spécifiée, elle a par défaut la valeur

1.



Activité de TP

Activité en ligne : Configuration de routes statiques

Au cours de ce TP, l'étudiant va apprendre à configurer des routes statiques.

6.1 Introduction au routage statique

6.1.4 Configuration de l'acheminement par défaut

Les routes par défaut permettent de router des paquets dont les destinations ne correspondent à aucune autre route de la table de routage. Les routeurs sont généralement configurés avec une route par défaut pour le trafic destiné à Internet, puisqu'il est souvent incommode et inutile de maintenir des routes vers tous les réseaux d'Internet. Une route par défaut est en fait une route statique spéciale qui utilise le format:

```
ip route 0.0.0.0 0.0.0.0 [adresse de saut suivant | interface de sortie ]
```

Le masque 0.0.0.0, lorsque lié par un ET logique à l'adresse IP de destination du paquet à acheminer, générera toujours le réseau 0.0.0.0. Si le paquet ne correspond pas à une route plus spécifique de la table de routage, il sera acheminé vers le réseau 0.0.0.0.

Pour configurer des routes par défaut, procédez comme suit:

Étape 1 Passez en mode de configuration globale.

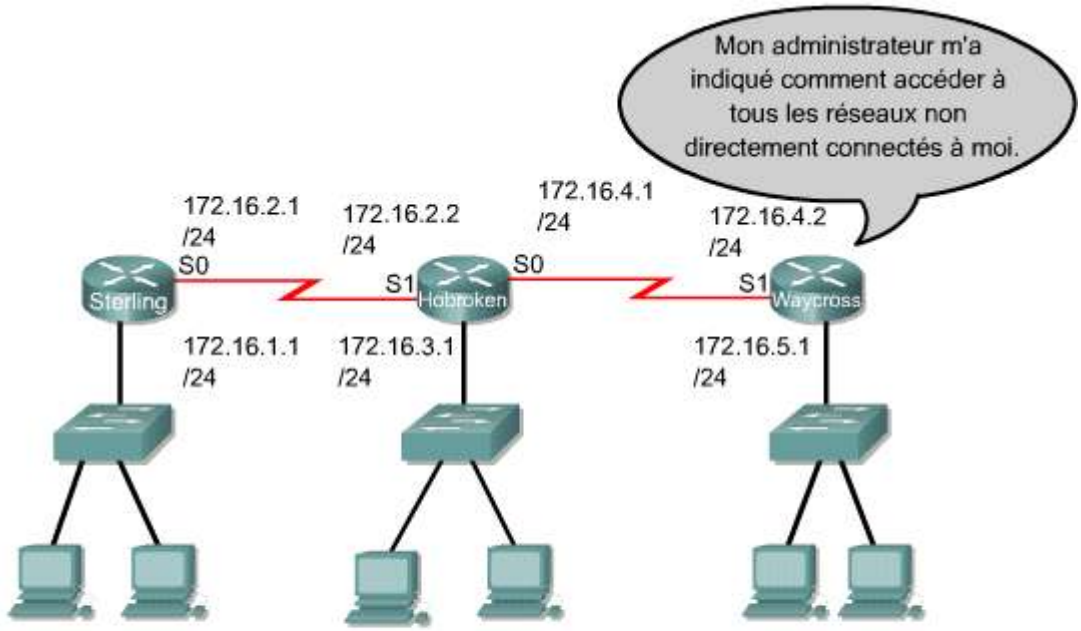
Étape 2 Entrez la commande **ip route** avec 0.0.0.0 comme préfixe et 0.0.0.0 comme masque. L'option adresse de la route par défaut peut être soit l'interface du routeur local qui permet de se connecter vers l'extérieur, soit l'adresse IP du routeur dans le saut suivant

Étape 3 Quittez le mode de configuration globale.

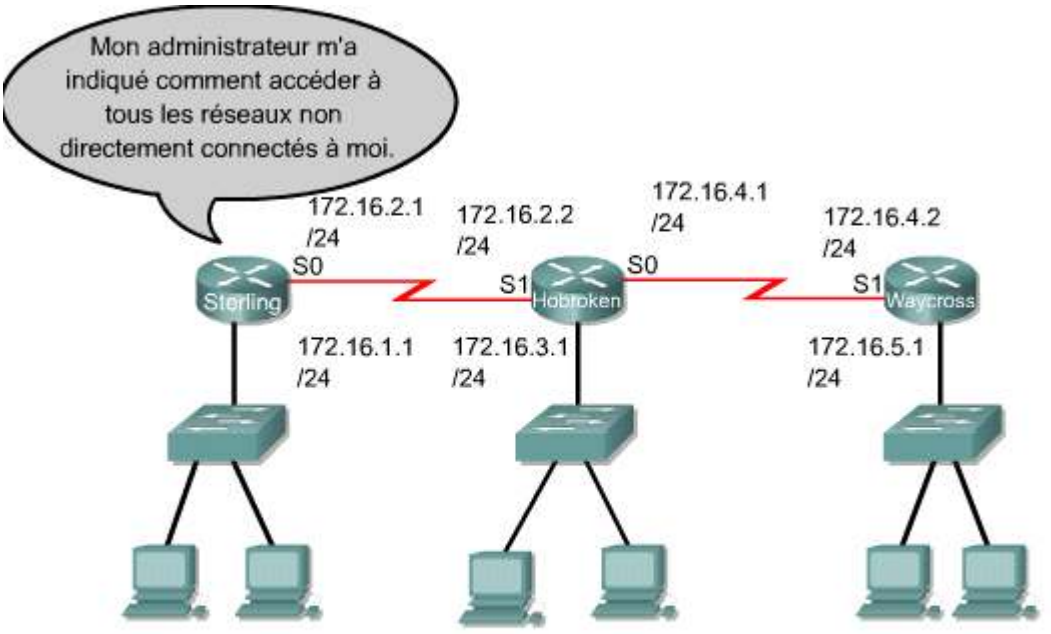
Étape 4 Enregistrez la configuration courante en mémoire NVRAM en utilisant la commande **copy running-config startup-config**.

Dans la section Configuration de routes statiques, les routes statiques ont été configurées sur le routeur Hoboken pour rendre accessibles les réseaux 172.16.1.0 sur Sterling et 172.16.5.0 sur Waycross. Il doit à présent être possible d'acheminer des paquets vers ces deux réseaux à partir d'Hoboken. Cependant, ni Sterling ni Waycross ne sauront comment retourner des paquets à un réseau non directement connecté. Une route statique pourrait être configurée sur Sterling et Waycross, pour chacun des réseaux de destination non directement connectés. Cela ne serait pas une solution assez évolutive dans le cas d'un grand réseau.

Le routeur Sterling se connecte à tous les réseaux non directement connectés via l'interface série 0. Le routeur Waycross a uniquement une connexion à tous les réseaux non directement connectés, via l'interface série 1. Une route par défaut sur Sterling et Waycross assurera le routage de tous les paquets qui sont destinés aux réseaux non directement connectés. 1 2




```
Waycross(config)#ip route 0.0.0.0  0.0.0.0 S1
```
Cette commande pointe vers tous les réseaux non directement connectés




```
Sterling(config)#ip route 0.0.0.0  0.0.0.0 S0
```
Cette commande pointe vers tous les réseaux non directement connectés

Activité de TP

Activité en ligne : Configuration de l'acheminement par défaut

Au cours de ce TP, les étudiants vont configurer une route statique par défaut.

6.1 Introduction au routage statique

6.1.5 Vérification de la configuration de route statique

Une fois les routes statiques configurées, il est important de vérifier qu'elles figurent dans la table de routage et que le routage fonctionne comme prévu. La commande **`show running-config`** permet de visualiser la configuration courante en mémoire RAM afin de vérifier que la route statique a été entrée correctement. La commande **`show ip route`** permet quant à elle de s'assurer que la route statique figure bien dans la table de routage.

Pour vérifier la configuration des routes statiques, procédez comme suit:

- En mode privilégié, entrez la commande **`show running-config`** pour visualiser la configuration courante.
- Vérifiez que la route statique a été correctement entrée. Si la route n'est pas correcte, il vous faudra repasser en mode de configuration globale pour supprimer la route statique incorrecte et en insérer une correcte.
- Entrez la commande **`show ip route`**.
- Vérifiez que la route qui a été configurée figure dans la table de routage.

```
Router#show running-config
Current configuration : 953 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
memory-size iomem 15
ip subnet-zero
no ip finger
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 2 in
!
interface Serial0/0
 ip address 200.200.2.1 255.255.255.0
 ip access-group 101 in
!
access-list 2 deny   172.16.1.1
access-list 2 permit 172.16.1.0 0.0.0.255
access-list 2 deny   172.16.0.0 0.0.255.255
access-list 2 permit 172.0.0.0 0.255.255.255
```

```
access-list 101 permit tcp 192.168.6.0 0.0.0.255 any
eq telnet
access-list 101 permit tcp 192.168.6.0 0.0.0.255 any
eq ftp
!
line con 0
 transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end
```

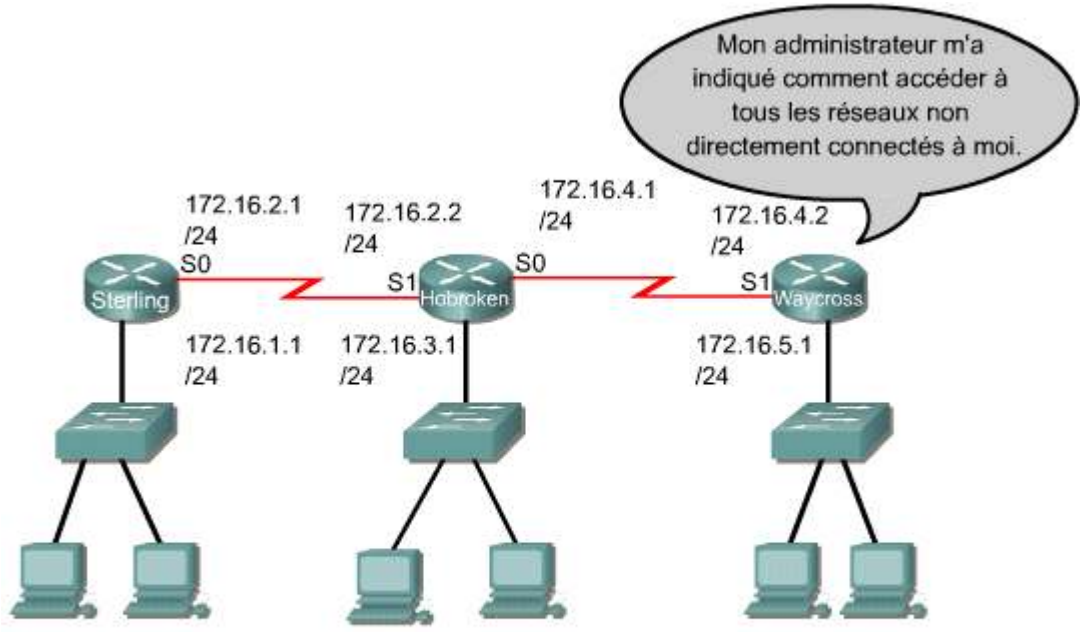
```
Router#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP,
       M - mobile, B - BGP, D - EIGRP,
       EX - EIGRP external, O - OSPF,
       IA - OSPF inter area,
       N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2,
       E1 - OSPF external type 1,
       E2 - OSPF external type 2,
       E - EGP, i - IS-IS, L1 - IS-IS level-1,
       L2 - IS-IS level-2, ia - IS-IS inter area,
       * - candidate default, U - per-user static
route,
       o - ODR, P - periodic downloaded static route


Gateway of last resort is not set


C    200.200.2.0/24 is directly connected, Serial0/0
S    172.16.0.0/16 [1/0] via 200.200.2.2

C    192.168.1.0/24 is directly connected,
FastEthernet0/0
```

Activité de TP

Activité en ligne : Vérification de la configuration d'une route statique

Au cours de ce TP, les étudiants vont utiliser les commandes show pour vérifier la configuration de la route statique par défaut qui a été créée au cours du précédent TP.

Dans la section «Configuration des routes statiques», nous avons configuré des routes statiques sur le routeur Hoboken pour rendre accessibles les réseaux 172.16.1.0 sur Sterling et 172.16.5.0 sur Waycross 1

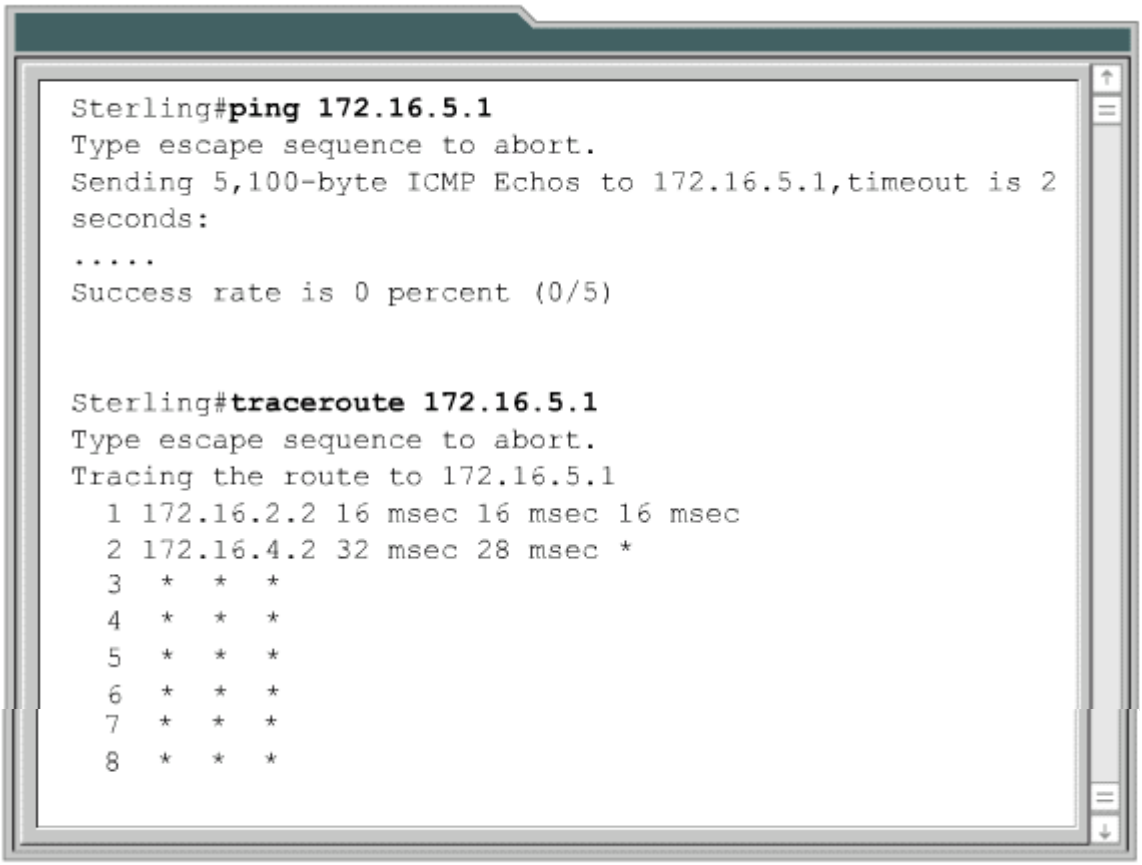


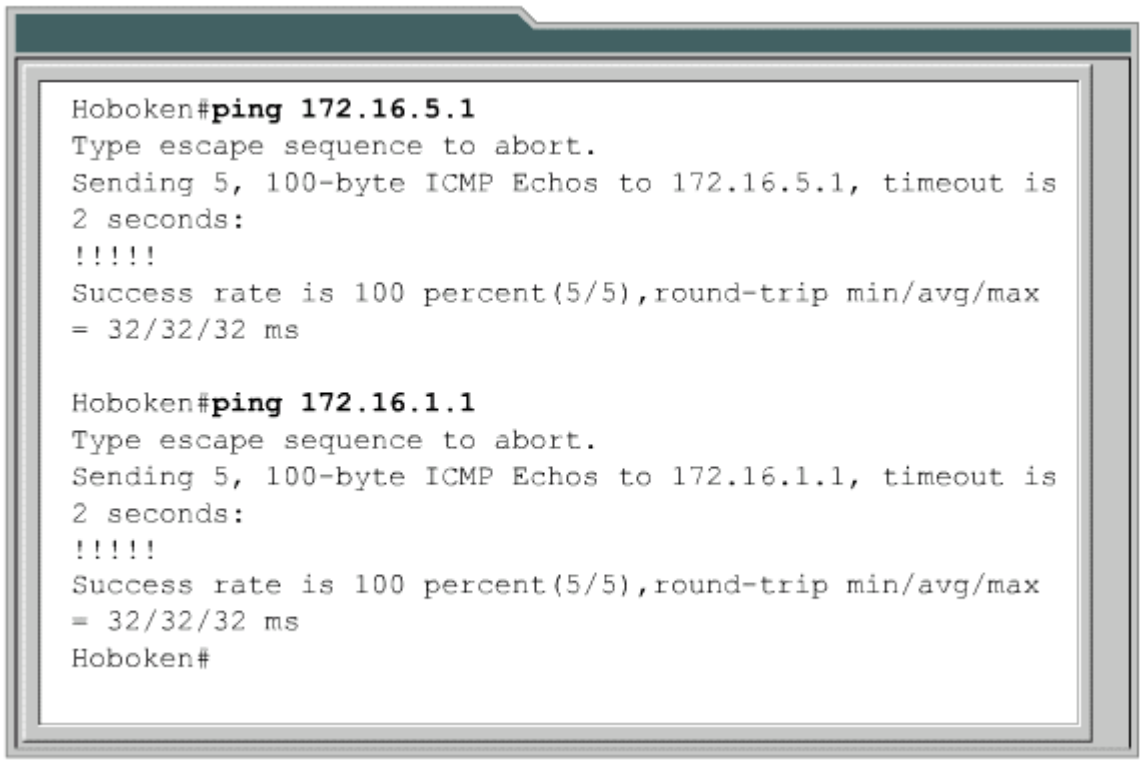

```
Waycross(config)#ip route 0.0.0.0  0.0.0.0 S1
```
Cette commande pointe vers tous les réseaux non directement connectés

Si nous utilisons cette configuration, les noeuds du réseau 172.16.1.0 de Sterling ne peuvent atteindre ceux du réseau 172.16.5.0. À partir du mode privilégié sur le routeur Sterling, utilisez la commande **ping** vers un nœud du réseau 172.16.5.0. Cette commande échoue. 2

```
Hoboken#show ip route
Codes:C-connected,S-static,I-IGRP,R-RIP,M-mobile,B-BGP
D-EIGRP,EX-EIGRP external,O- OSPF,IA-OSPF inter area
N1-OSPF NSSA external type 1,N2-OSPF NSSA external type2
E1-OSPF external type 1,E2-OSPF external type 2, E - EGP
i-IS-IS,L1-IS-IS level-1,L2-IS-IS level-2,ia-IS-IS inter
area
* -candidate default, U - per-user static route, o - ODR
P -periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 5 subnets
C       172.16.4.0 is directly connected, Serial0
S       172.16.5.0 is directly connected, Serial0
S       172.16.1.0 is directly connected, Serial1
C       172.16.2.0 is directly connected, Serial1
C       172.16.3.0 is directly connected, FastEthernet0
Hoboken#
```

Maintenant utilisez la commande **traceroute** de Sterling vers l'adresse qui a été utilisée précédemment avec la commande **ping**. Prenez note de l'endroit où la commande **traceroute** échoue. Elle indique que le paquet ICMP a été renvoyé depuis Hoboken mais pas depuis Waycross. 2 Le problème se situe donc au niveau d'Hoboken ou de Waycross. Établissez une connexion Telnet avec le routeur Hoboken. Tentez à nouveau d'exécuter une commande **ping** sur le noeud du réseau 172.16.5.0 connecté au routeur Waycross. Elle doit aboutir, car Hoboken est directement connecté à Waycross. 3





Activité de TP

Exercice : Configuration de routes statiques

Au cours de ce TP, les étudiants vont utiliser les commandes show pour vérifier la configuration de la route statique par défaut qui a été créée au cours du précédent TP.

Activité de TP

Activité en ligne : Routes statiques

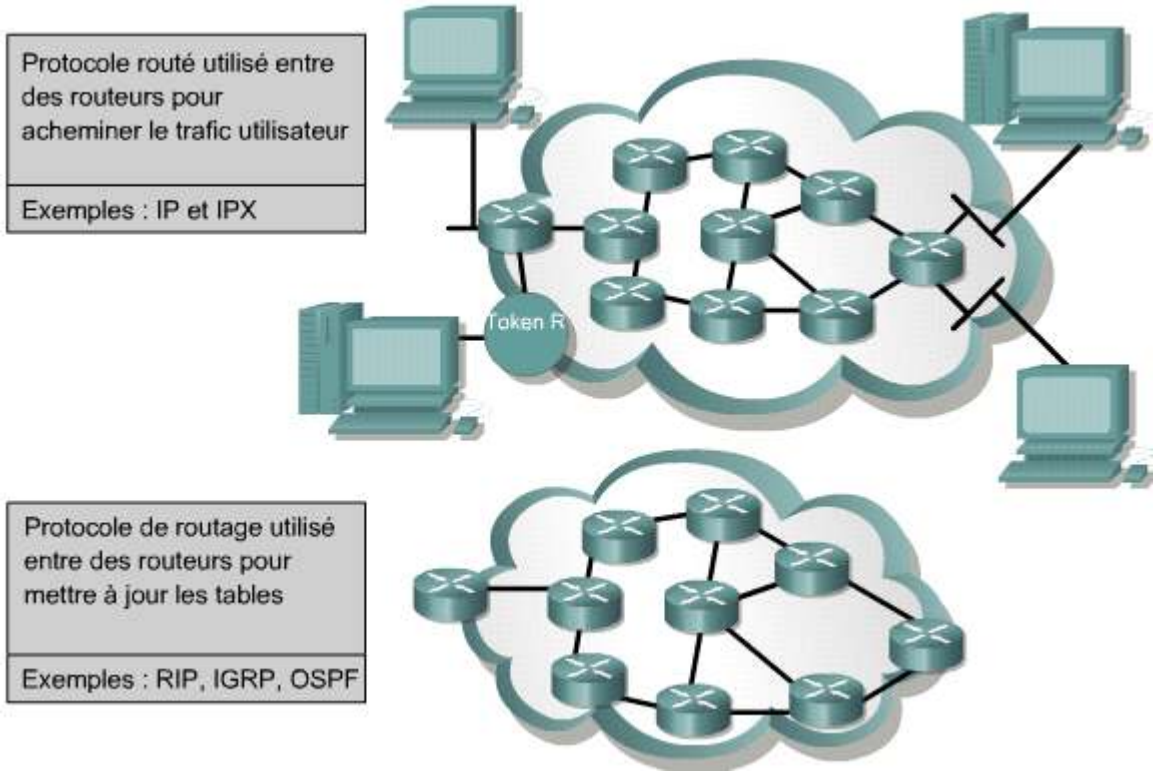
Au cours de ce TP, les étudiants vont configurer des routes statiques entre des routeurs pour permettre le transfert de données sans utiliser de protocoles de routage dynamiques.

6.2 Vue d'ensemble du routage dynamique

6.2.1 Introduction aux protocoles de routage

Les protocoles de routage différent des protocoles routés sur le plan de la fonction comme de la tâche.

Un protocole de routage est le système de communication utilisé entre les routeurs. Le protocole de routage permet à un routeur de partager avec d'autres routeurs des informations sur les réseaux qu'il connaît, ainsi que sur leur proximité avec d'autres routeurs. Les informations qu'un routeur reçoit d'un autre routeur, à l'aide d'un protocole de routage, servent à construire et à mettre à jour une table de routage. 1



Exemples:

- Protocole d'informations de routage (RIP)
- Protocole IGRP (*Interior Gateway Routing Protocol*)
- Protocole EIGRP (Enhanced Interior Gateway Routing Protocol)
- Protocole OSPF (Open Shortest Path First)

Un protocole routé sert à diriger le trafic utilisateur. Il fournit suffisamment d'informations dans son adresse de couche réseau pour permettre l'acheminement d'un paquet d'un hôte à un autre en fonction de la méthode d'adressage.

Exemples :

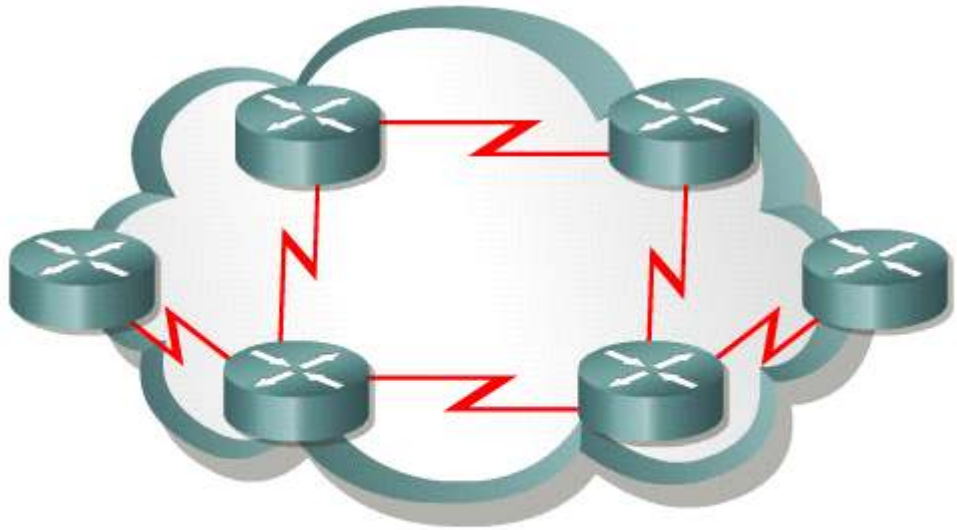
- Le protocole Internet (IP)
- Le protocole IPX (Internetwork Packet Exchange)

6.2 Vue d'ensemble du routage dynamique

6.2.2 Systèmes autonomes

Un système autonome est un ensemble de réseaux gérés par un administrateur commun et partageant une stratégie de routage commune. Pour le monde extérieur, un système autonome est perçu comme une entité unique. Il peut être exécuté par un ou plusieurs opérateurs tout en présentant au monde extérieur une vue cohérente du routage.

L'InterNIC (*Internet Network Information Center*), un fournisseur de services ou encore un administrateur attribue un numéro d'identification à chaque système autonome. Ce numéro est un nombre à 16 bits. Les protocoles de routage, tels que l'IGRP de Cisco, nécessitent l'attribution d'un numéro de système autonome unique.



Routeurs sous administration commune

6.2 Vue d'ensemble du routage dynamique

6.2.3 Objet d'un protocole de routage et de systèmes autonomes

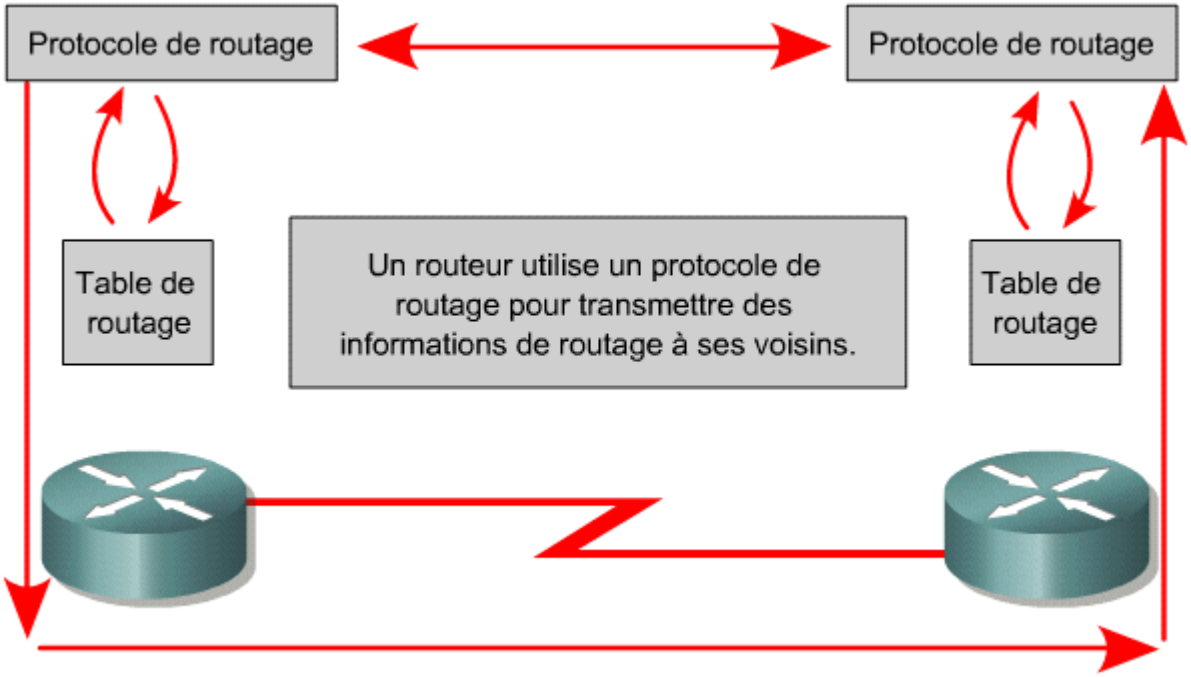
L'objet d'un protocole de routage est de construire et mettre à jour la table de routage. Cette table contient les réseaux acquis et les ports associés à ces réseaux. Les routeurs utilisent des protocoles de routage pour gérer des informations reçues d'autres routeurs, les informations acquises de la configuration de ces propres interfaces, ainsi que des routes configurées manuellement.

Le protocole de routage prend connaissance de toutes les routes disponibles. ll insère les meilleures routes dans la table de routage et supprime celles qui ne sont plus valides. Le routeur utilise les informations de la table de routage pour transmettre les paquets de protocole routé.

L'algorithme de routage est une composante essentielle du routage dynamique. Chaque fois que la topologie du réseau est modifiée en raison de la croissance, d'une reconfiguration ou d'une panne, la base de connaissances du réseau doit également être modifiée. La base de connaissances du réseau doit refléter une vue juste et cohérente de la nouvelle topologie.

Lorsque tous les routeurs d'un interréseau reposent sur les mêmes connaissances, on dit de l'interréseau qu'il a convergé. Une convergence rapide est préférable, car elle réduit la période au cours de laquelle les routeurs prennent des décisions de routage incorrectes ou inefficaces.

Les systèmes autonomes (AS) assurent la division de l'interréseau global en réseaux plus petits et plus faciles à gérer. Chaque système autonome possède son propre ensemble de règles et de politiques et un numéro AS unique qui le distinguera des autres systèmes autonomes à travers le monde.



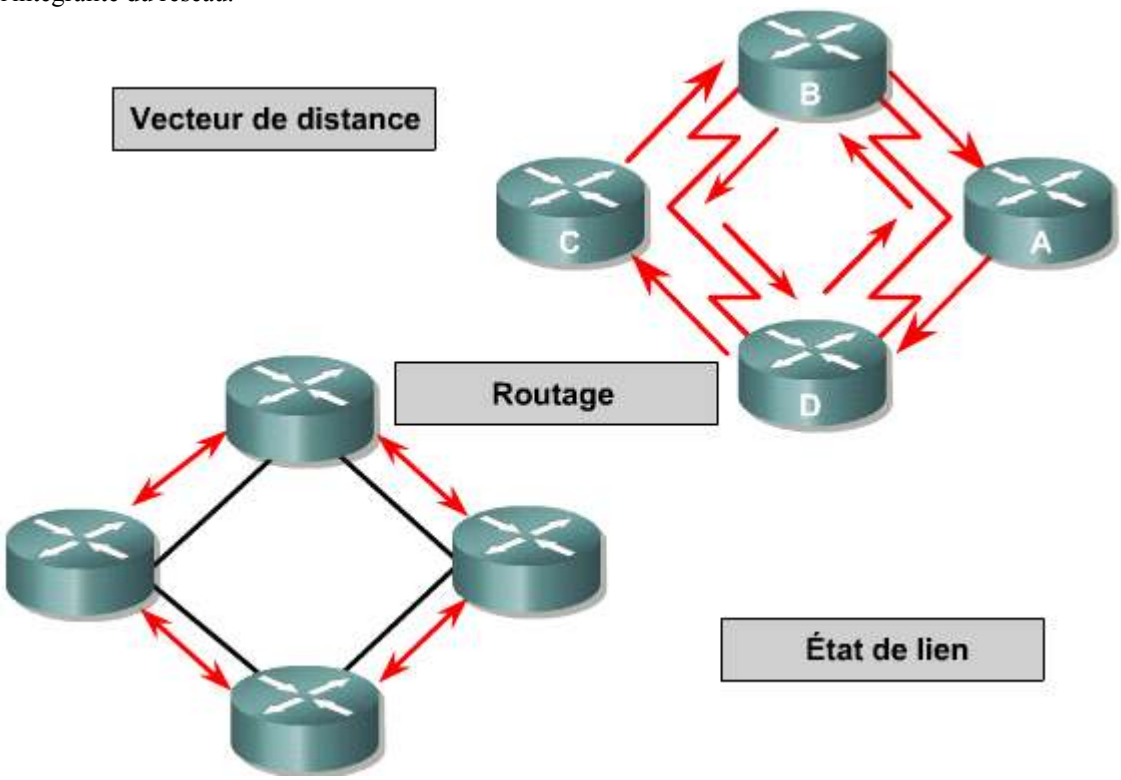
6.2 Vue d'ensemble du routage dynamique

6.2.4 Identification des classes des protocoles de routage

La plupart des algorithmes de routage peuvent être rangés dans l'une des catégories suivantes:

- vecteur de distance
- état de liens

Le routage à vecteur de distance détermine la direction (vecteur) et la distance jusqu'à une liaison quelconque de l'interréseau. L'approche à état de liens, également appelée routage par le chemin le plus court, recrée la topologie exacte de l'intégralité du réseau.

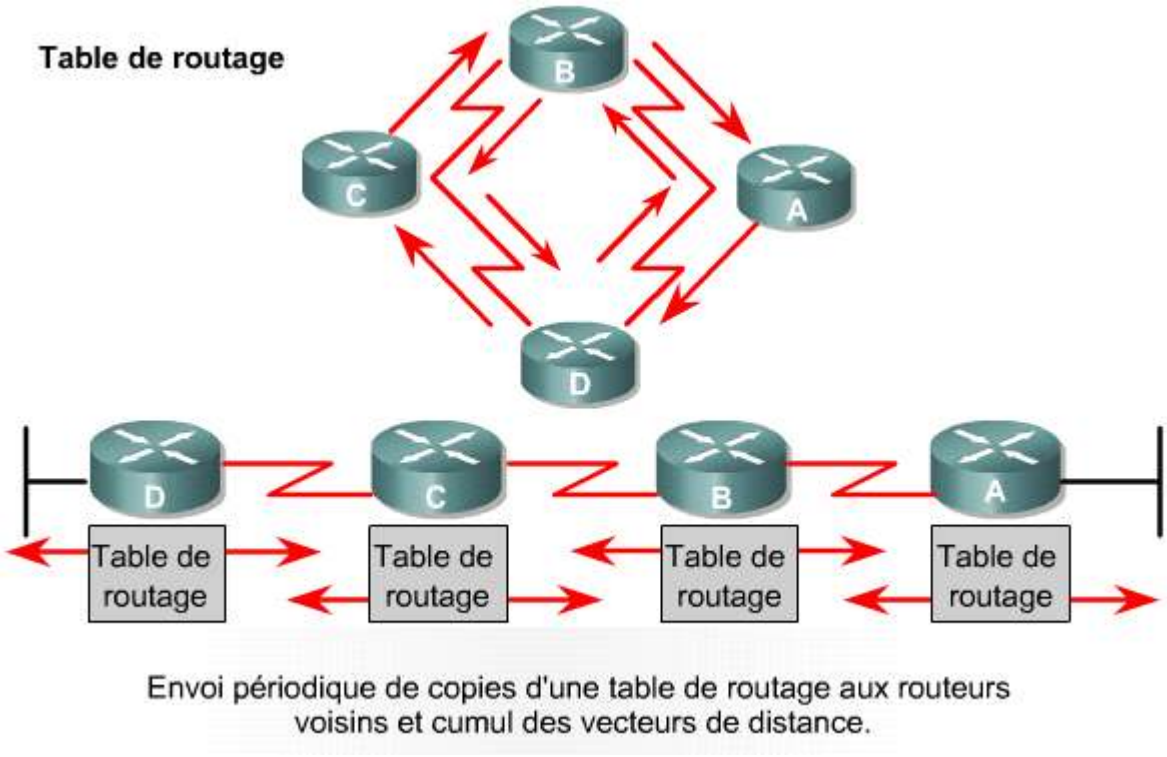


6.2 Vue d'ensemble du routage dynamique

6.2.5 Fonctions du protocole de routage à vecteur de distance

Les algorithmes de routage à vecteur de distance transmettent régulièrement des copies de table de routage d'un routeur à l'autre. Ces mises à jour régulières entre les routeurs permettent de communiquer les modifications topologiques. Les algorithmes de routage à vecteur de distance sont également appelés algorithmes Bellman-Ford.

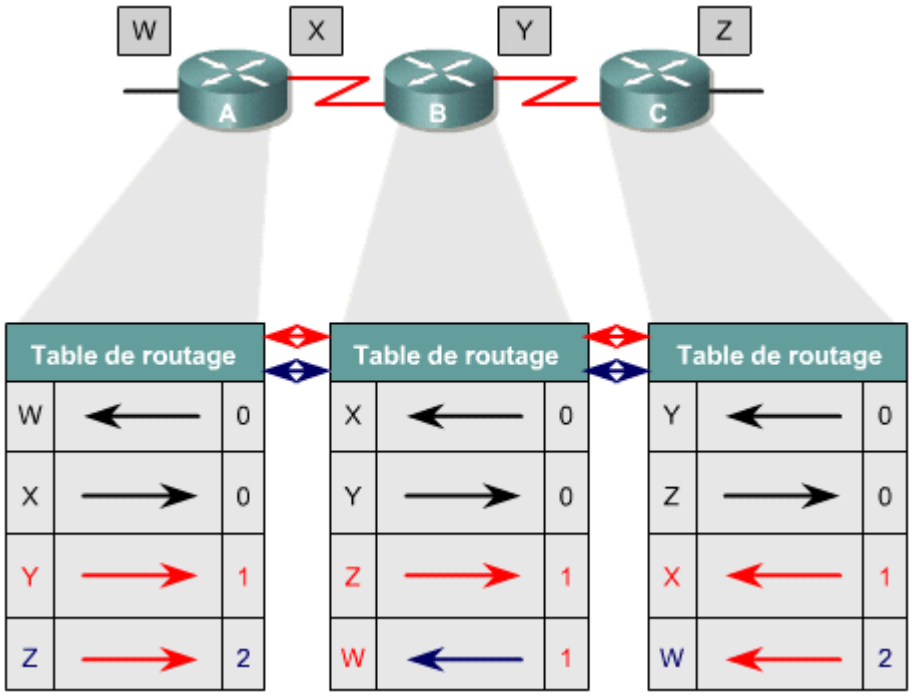
Chaque routeur reçoit une table de routage des routeurs voisins auxquels il est directement connecté. 1Le routeur B reçoit des informations du routeur A. Le routeur B ajoute un nombre de vecteurs (par exemple, un nombre de sauts) qui allonge le vecteur de distance. Ensuite, le routeur B transmet la nouvelle table de routage à son voisin, le routeur C. La même procédure est répétée étape par étape dans toutes les directions entre les routeurs directement adjacents.



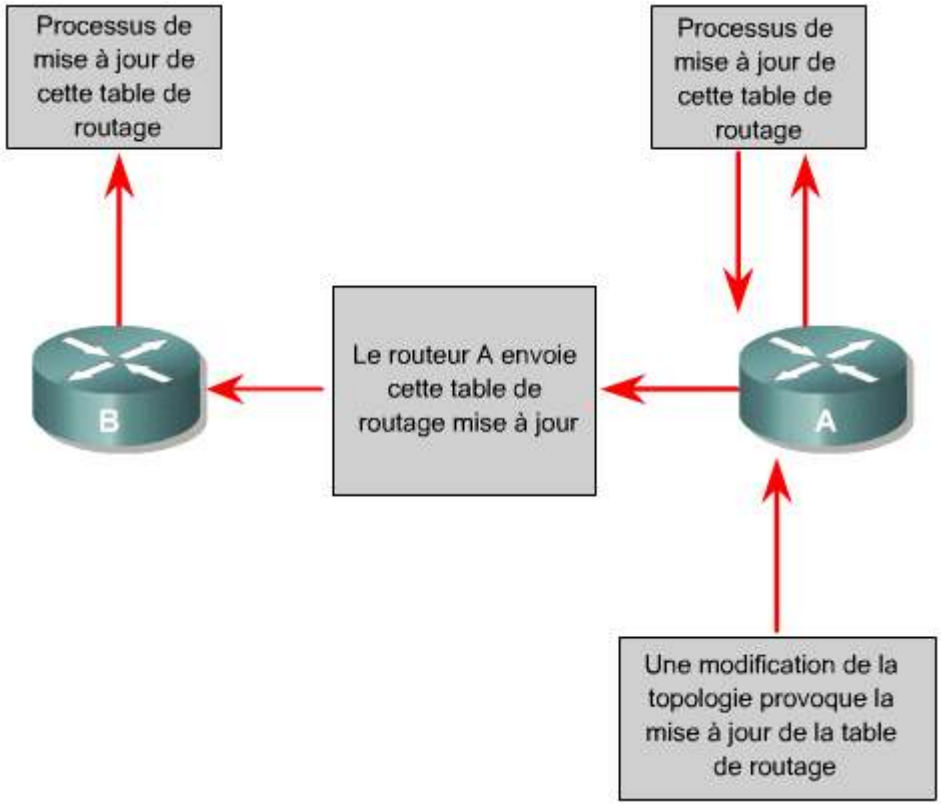
Envoi périodique de copies d'une table de routage aux routeurs voisins et cumul des vecteurs de distance.

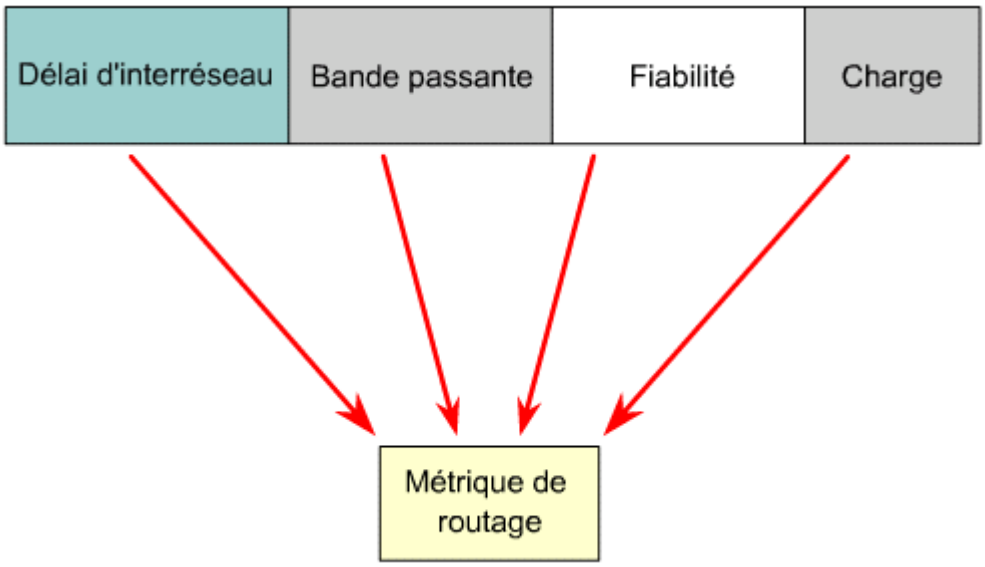
L'algorithme cumule les distances afin de tenir à jour la base de données contenant les informations sur la topologie du réseau. Cependant, les algorithmes de routage à vecteur de distance ne permettent pas à un routeur de connaître la topologie exacte d'un interréseau, étant donné que chaque routeur voit uniquement ses voisins.

Chaque routeur utilisant le routage à vecteur de distance commence par identifier ses voisins. 2La distance entre l'interface et chaque réseau directement connecté est égale à 0. Au fur et à mesure que le processus de découverte par vecteur de distance se poursuit, les routeurs découvrent le meilleur chemin menant aux réseaux de destination sur la base des informations reçues de chacun de leurs voisins. Le routeur A prend connaissance des autres réseaux grâce aux informations qu'il reçoit du routeur B. Chaque entrée de la table de routage pour chaque réseau correspond à un vecteur de distance cumulé, lequel indique la distance au réseau dans une direction donnée.



Lorsque la topologie change, les tables de routage sont mises à jour. Comme dans le cas du processus de découverte de réseau, la mise à jour des modifications topologiques s'effectue étape par étape, d'un routeur à l'autre. 3 Les algorithmes à vecteur de distance prévoient que chaque routeur transmettra aux routeurs voisins l'intégralité de sa table de routage. Les tables de routage contiennent des informations sur le coût total du chemin (défini par sa métrique) et l'adresse logique du premier routeur sur le chemin menant à chaque réseau contenu dans la table. 4





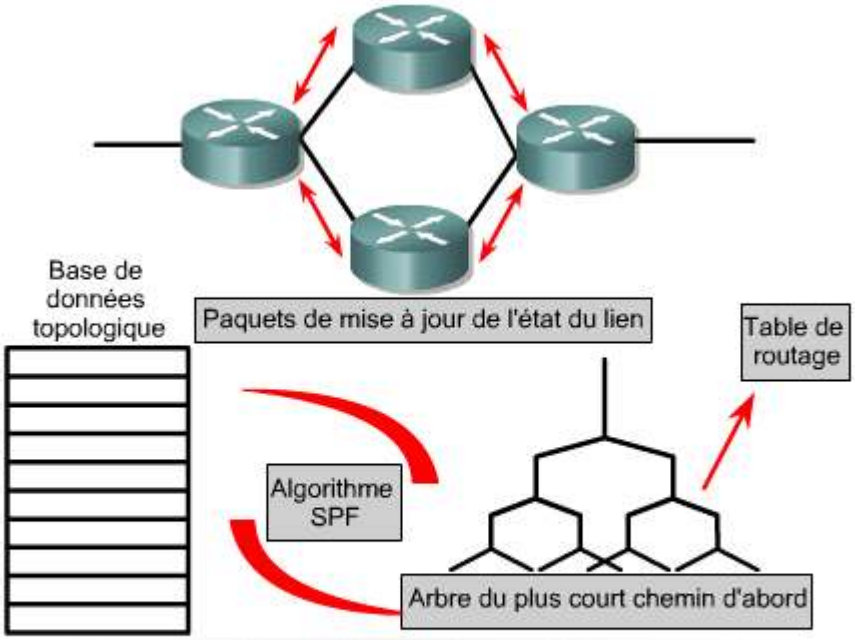
On pourrait comparer un vecteur de distance à la signalisation que l'on trouve aux croisements routiers. Un panneau pointe vers une destination et indique la distance à parcourir pour y parvenir. Plus loin sur la route nationale, un autre panneau montre la destination et indique cette fois une distance plus courte. Tant que la distance diminue, le trafic est sur le bon chemin.

6.2 Vue d'ensemble du routage dynamique

6.2.6 Fonctions du protocole de routage à état de liens

Le deuxième algorithme de base utilisé pour le routage est l'algorithme à état de liens. Ces algorithmes sont également appelés algorithme de Dijkstra ou algorithme SPF (shortest path first ou du plus court chemin d'abord). Ils gèrent une base de données complexe d'informations topologiques. L'algorithme à vecteur de distance comprend des informations non spécifiques sur les réseaux distants et ne fournit aucune information sur les routeurs distants. Un algorithme de routage à état de liens gère une base de connaissances complète sur les routeurs distants et leurs interconnexions.

Le routage à état de liens utilise les éléments suivants: 1



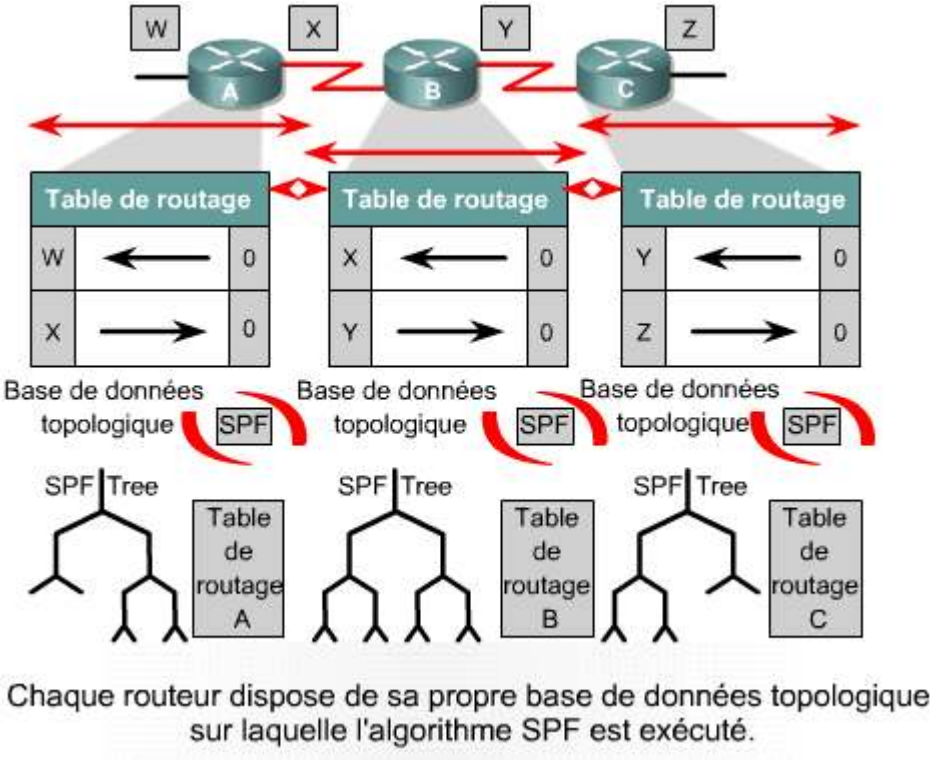
Les routeurs envoient des LSA à leurs voisins. Les LSA sont utilisées pour créer une base de données topologique. L'algorithme SPF est utilisé pour calculer l'arbre du plus court chemin d'abord dans lequel la racine est le routeur lui même. Une table de routage est ensuite créée.

- **Mises à jour de routage à état de liens (LSA) –** Une mise à jour de routage à état de liens (LSA) est un petit paquet d'informations de routage qui est transmis entre les routeurs.
- **Base de données topologique –** Une base de données topologique est un ensemble d'informations rassemblées à partir des mises à jour de routage à état de liens.
- **Algorithme SPF –** L'algorithme du plus court chemin d'abord (SPF) est un calcul effectué sur la base de données qui génère un arbre SPF.
- **Tables de routage –** Une liste des chemins et des interfaces connus.

Processus de découverte du réseau pour le routage à état de liens

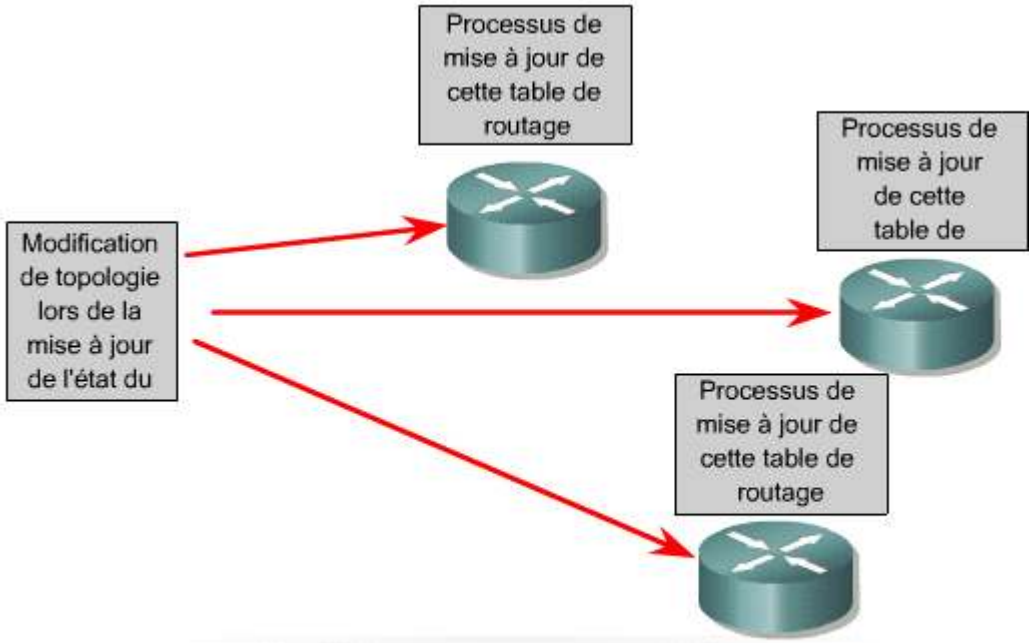
Les mises à jour de routage à état de liens sont échangées entre routeurs en commençant par les réseaux directement connectés au sujets desquels ils sont directement informés. Parallèlement à ses homologues, chaque routeur génère une base de données topologiques comprenant toutes les mises à jour de routage à état de liens échangées.

L'algorithme du plus court chemin d'abord (SPF) calcule l'accessibilité aux réseaux. Le routeur génère cette topologie logique sous la forme d'un arbre dont il est la racine et qui comporte tous les chemins possibles menant à chaque réseau de l'interréseau utilisant le protocole à état de liens. Ensuite, il trie ces chemins sur la base du chemin le plus court. Le routeur répertorie dans sa table de routage les meilleurs chemins et les interfaces menant aux réseaux de destination. Il met également à jour d'autres bases de données contenant des éléments de topologie et les détails relatifs à leur état. 2



Chaque routeur dispose de sa propre base de données topologique sur laquelle l'algorithme SPF est exécuté.

Le premier routeur informé de la modification de la topologie d'état de liens transmet l'information pour que tous les autres routeurs puissent l'utiliser pour des mises à jour. 3 Ainsi, les informations de routage communes sont envoyées à tous les routeurs de l'interréseau. Pour atteindre la convergence, chaque routeur effectue le suivi de ses routeurs voisins, du nom du routeur, de l'état de l'interface, ainsi que du coût de la liaison avec chaque voisin. Le routeur génère un paquet de mise à jour de routage (LSA) qui répertorie ces informations ainsi les noms des nouveaux voisins, les modifications relatives aux coûts de liaison et les liaisons qui ne sont plus valides. Le paquet LSA est ensuite transmis à tous les autres routeurs.



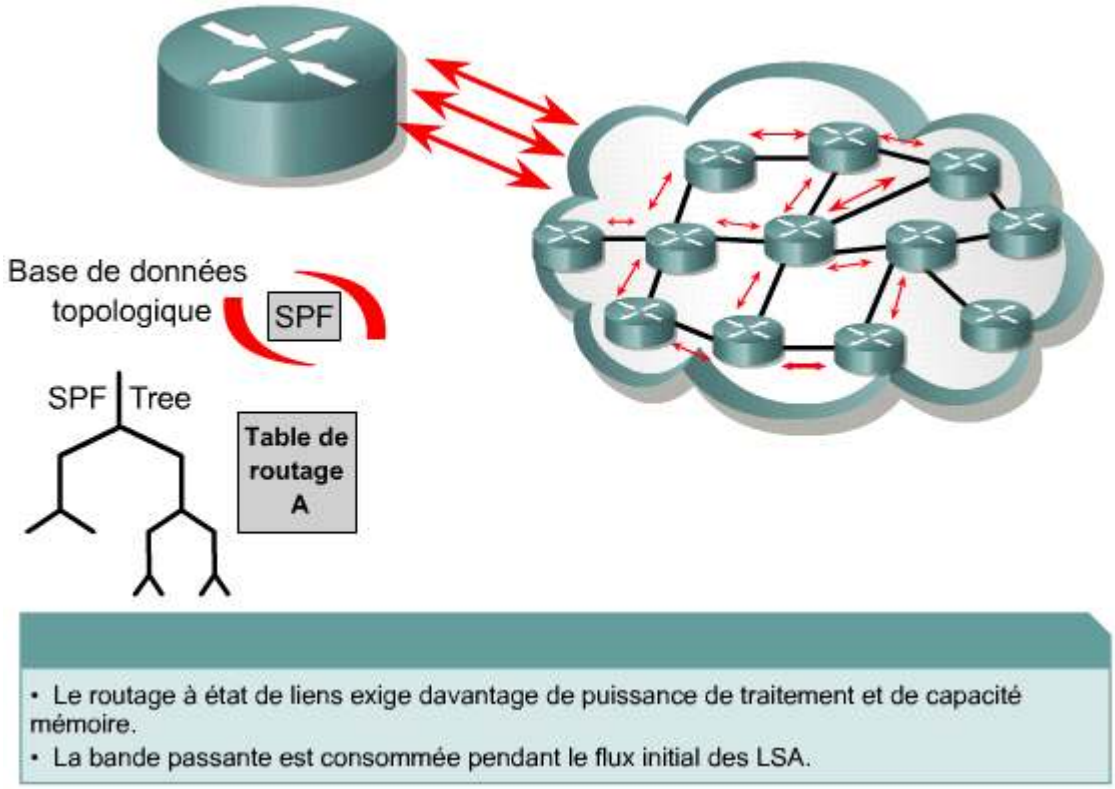
Chaque routeur dispose de sa propre base de données topologique sur laquelle l'algorithme SPF est exécuté.

Lorsque le routeur reçoit une LSA, la base de données est mise à jour avec les informations les plus récentes et il génère une carte de l'interréseau à l'aide des données accumulées et détermine les routes vers tous les autres réseaux à l'aide de l'algorithme du plus court chemin d'abord. Chaque fois qu'un paquet de mise à jour de routage à état de liens entraîne une modification dans la base de données d'état de liens, l'algorithme du plus court chemin d'abord recalcule les meilleurs chemins et met à jour la table de routage.

Considérations relatives au routage à état de liens:

- Surcharge du système
- Mémoire requise
- Consommation de bande passante

Les protocoles de routage à état de liens nécessitent davantage de mémoire et de capacités de calcul que les protocoles de routage à vecteur de distance. Les routeurs doivent disposer d'une mémoire suffisante pour stocker toutes les informations des différentes bases de données, l'arbre topologique et la table de routage. Le flux initial des paquets de mise à jour de routage à état de liens consomme de la bande passante. Durant le processus initial de découverte, tous les routeurs utilisant des protocoles de routage à état de liens transmettent les paquets de mise à jour aux autres routeurs. Cela a pour effet de submerger l'interréseau et de réduire de façon temporaire la bande passante disponible pour le trafic routé des données utilisateur. Par la suite, les protocoles de routage à état de liens ne nécessitent généralement qu'un minimum de bande passante pour envoyer les paquets de mise à jour reflétant les modifications topologiques. L'envoi peut être sporadique ou déclenché par un événement.



- Le routage à état de liens exige davantage de puissance de traitement et de capacité mémoire.
- La bande passante est consommée pendant le flux initial des LSA.

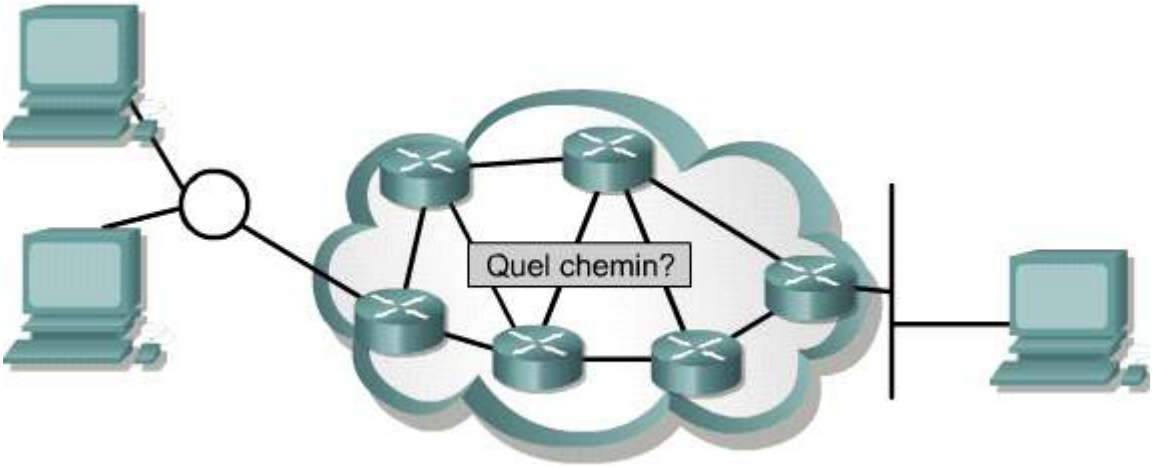
6.3 Vue d'ensemble des protocoles de routage

6.3.1 Détermination du chemin

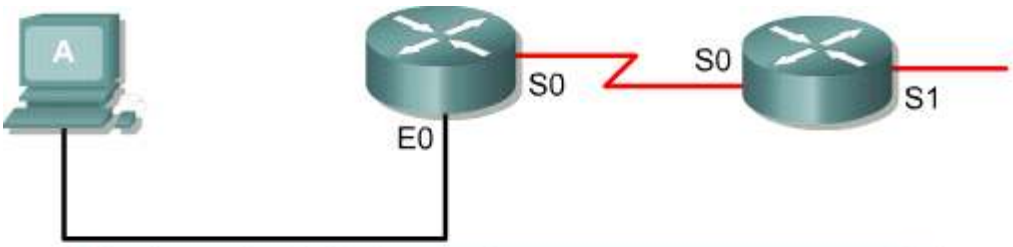
En règle générale, un routeur détermine le chemin que doit emprunter un paquet entre deux liaisons à l'aide des deux fonctions de base suivantes:

- la détermination du chemin,
- la commutation.

La détermination du chemin se produit au niveau de la couche réseau. La fonction de détermination de chemin permet à un routeur d'évaluer les chemins vers une destination donnée et de définir le meilleur chemin pour traiter un paquet. Le routeur se sert de la table de routage pour déterminer le meilleur chemin et transmet ensuite le paquet en utilisant la fonction de commutation. 1 – 4



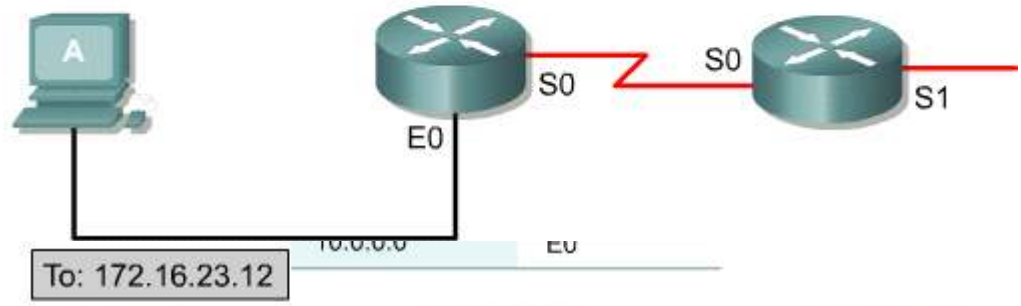
La couche 3 recherche le meilleur chemin dans l'interréseau.

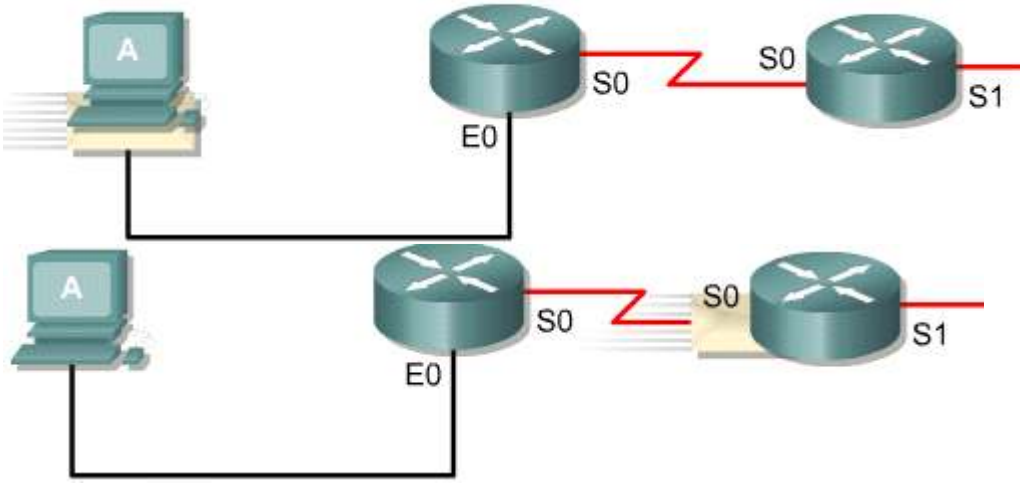


Fenêtre contextuelle (pop up)

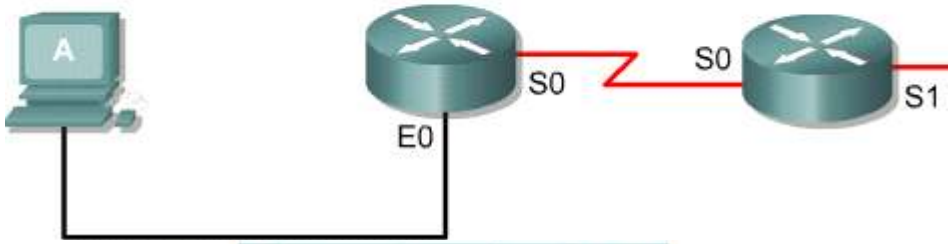
Une table de routage IP est constituée de paires " adresses réseau de destination et saut suivant ". Une entrée peut indiquer que pour atteindre le réseau 172.31.0.0, par exemple, le paquet doit être envoyé par l'interface S0. Dans le cadre du routage IP, les datagrammes IP parcourent l'interréseau un saut à la fois. À chaque saut, la destination suivante est calculée en faisant correspondre l'adresse de destination dans le datagramme à une interface de sortie. S'il n'y a aucune correspondance, le datagramme est envoyé au routeur par défaut.

Réseau de destination	Interface (Saut suiv.)
172.31.0.0	S0
172.19.0.0	--
192.168.1.0	--
10.0.0.0	E0



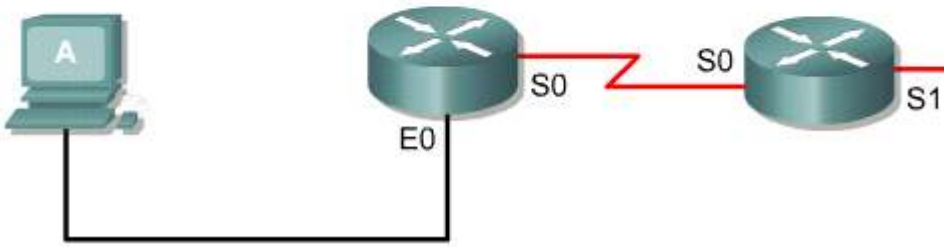


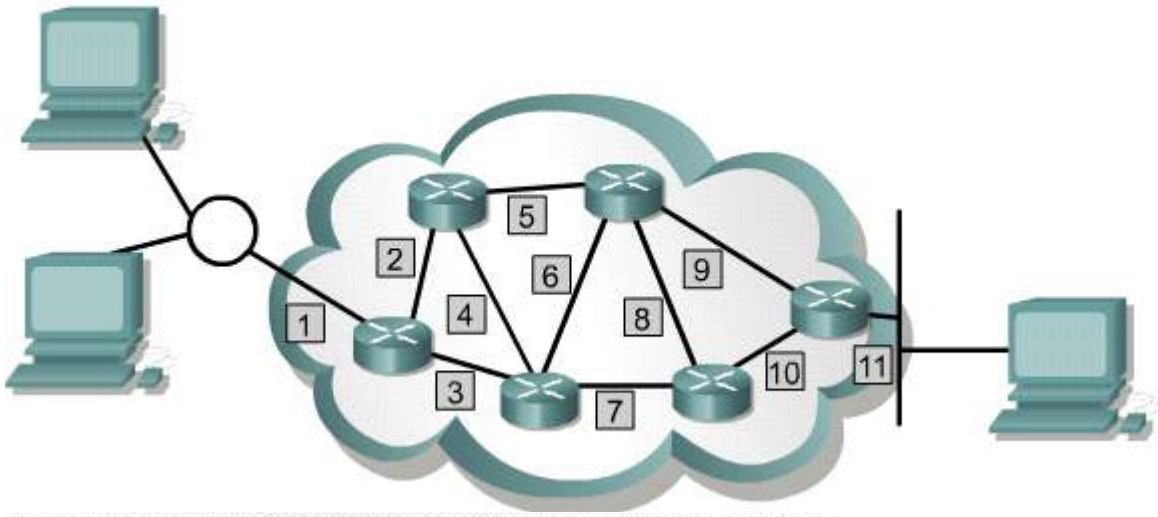
Réseau de destination	Interface (Saut suiv.)
172.16.0.0	S0
172.18.0.0	--
192.168.24.0	s0
Rout. par défaut	S1



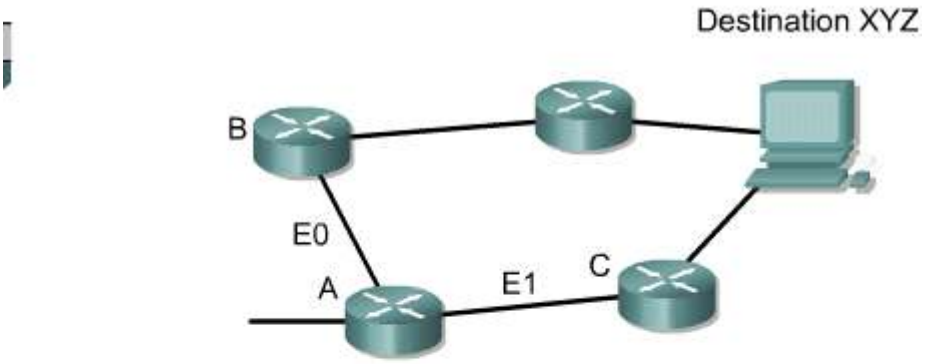
Réseau de destination	Interface (Saut suiv.)
172.16.0.0	S0
172.18.0.0	--
192.168.24.0	s0
Rout. par défaut	S1

Pas de corresp.



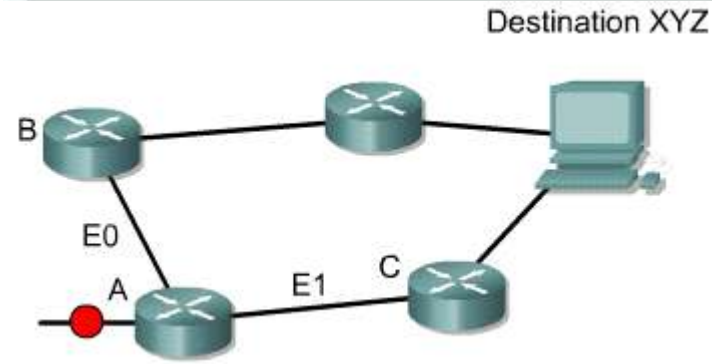


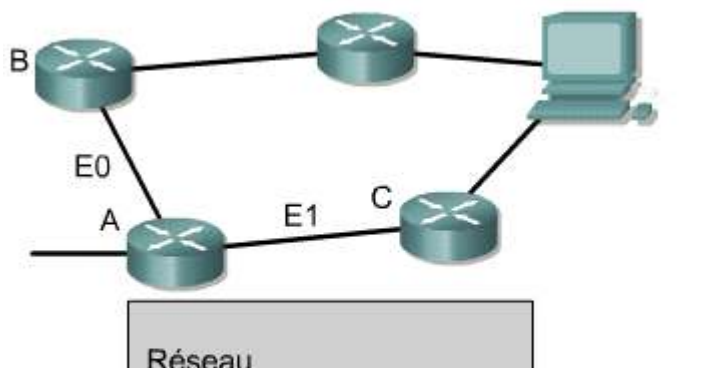
Les adresses représentent le chemin des connexions média.

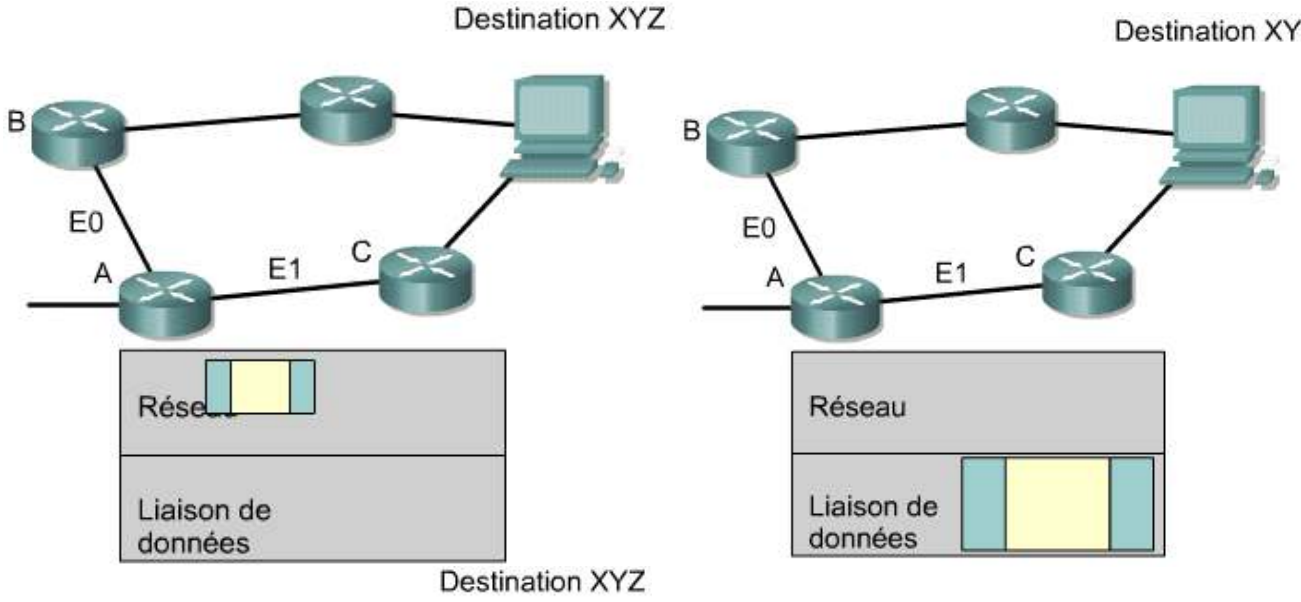


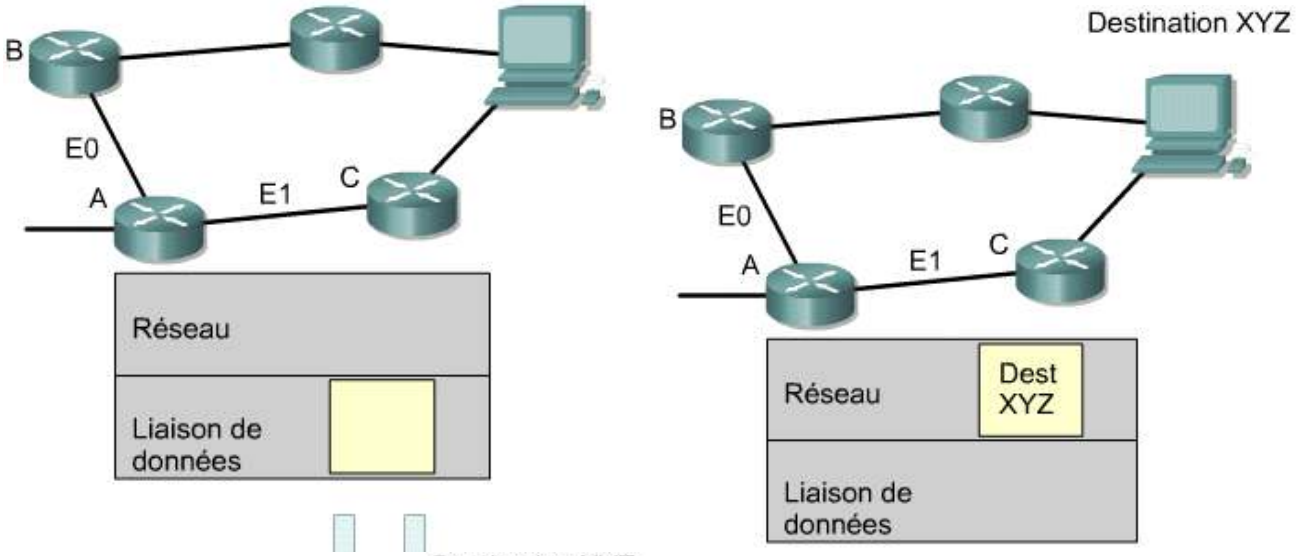
Fenêtre contextuelle (pop up)

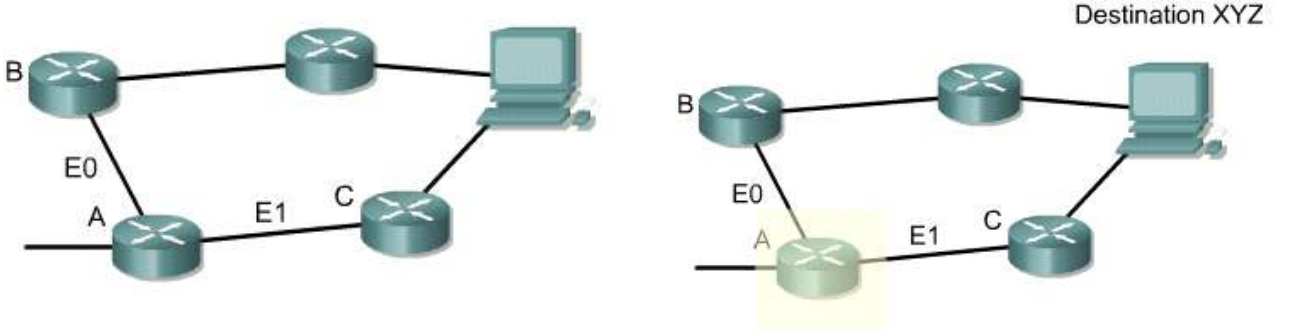
L'une des fonctions du routeur consiste à déterminer le chemin à utiliser pour transmettre une trame donnée. La trame arrive sur une interface du routeur. La trame de couche liaison de données est retirée et éliminée. Quant à la trame de couche réseau, elle est envoyée au processus de couche réseau approprié. L'en-tête de protocole réseau est alors examiné afin de déterminer la destination du paquet. Le processus de couche réseau consulte ensuite la table de routage, qui indique l'interface connectée au meilleur saut vers la destination. Le paquet est ensuite retransmis à la couche liaison de données, où il est encapsulé dans une nouvelle trame. Ensuite, il est placé en file d'attente afin d'être acheminé à l'interface appropriée. Enfin, la trame est insérée dans le réseau et voyage jusqu'au routeur du saut suivant, où le processus se répète.







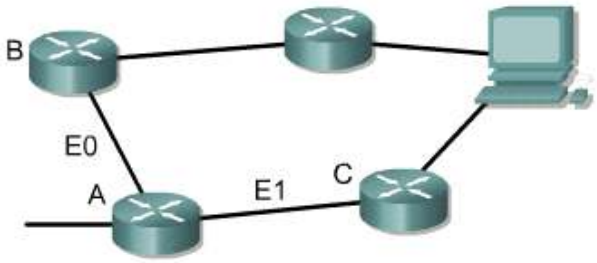




Interface	Souhaitable	Saut suiv.	Dest.
E1	+	Router C	XYZ
E0	-	Router B	XYZ

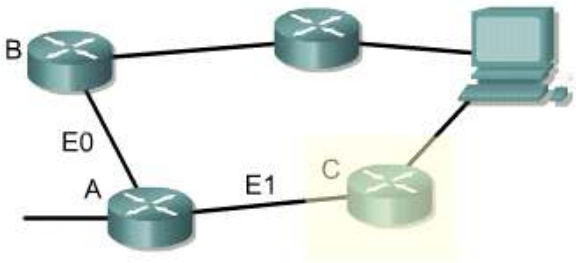
Interface	Souhaitable	Saut suiv.	Dest.
E1	+	Router C	XYZ
E0	-	Router B	XYZ

Destination XYZ



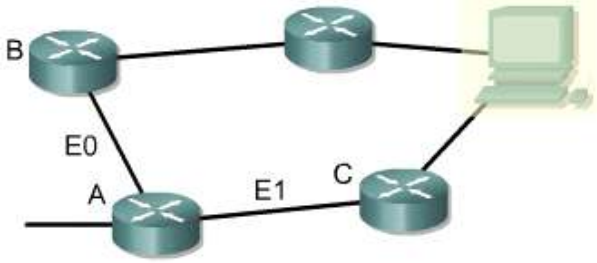
Interface	Souhaitable	Saut suiv.	Dest.
E1	+	Router C	XYZ
E0	-	Router B	XYZ

Destination XYZ



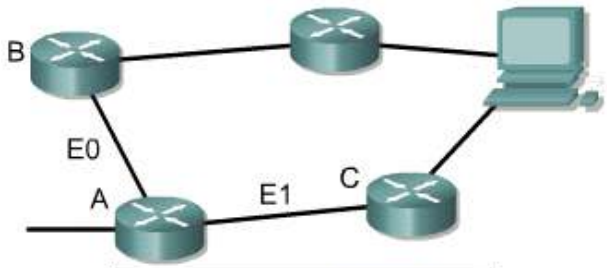
Interface	Souhaitable	Saut suiv.	Dest.
E1	+	Router C	XYZ
E0	-	Router B	XYZ

Destination XYZ

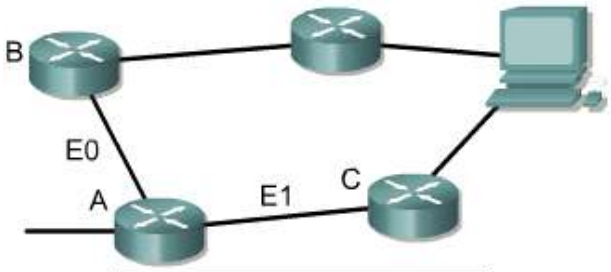


Interface	Souhaitable	Saut suiv.	Dest.
E1	+	Router C	XYZ
E0	-	Router B	XYZ

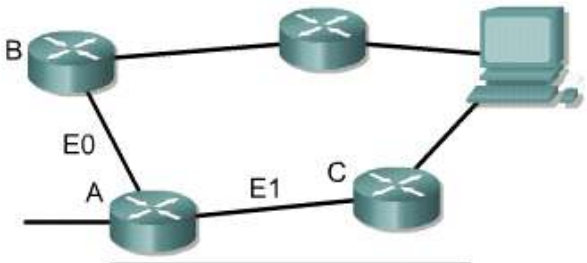
Destination XYZ

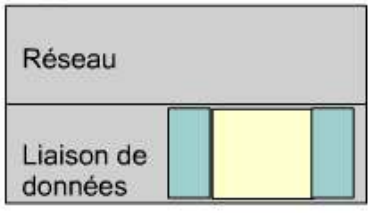


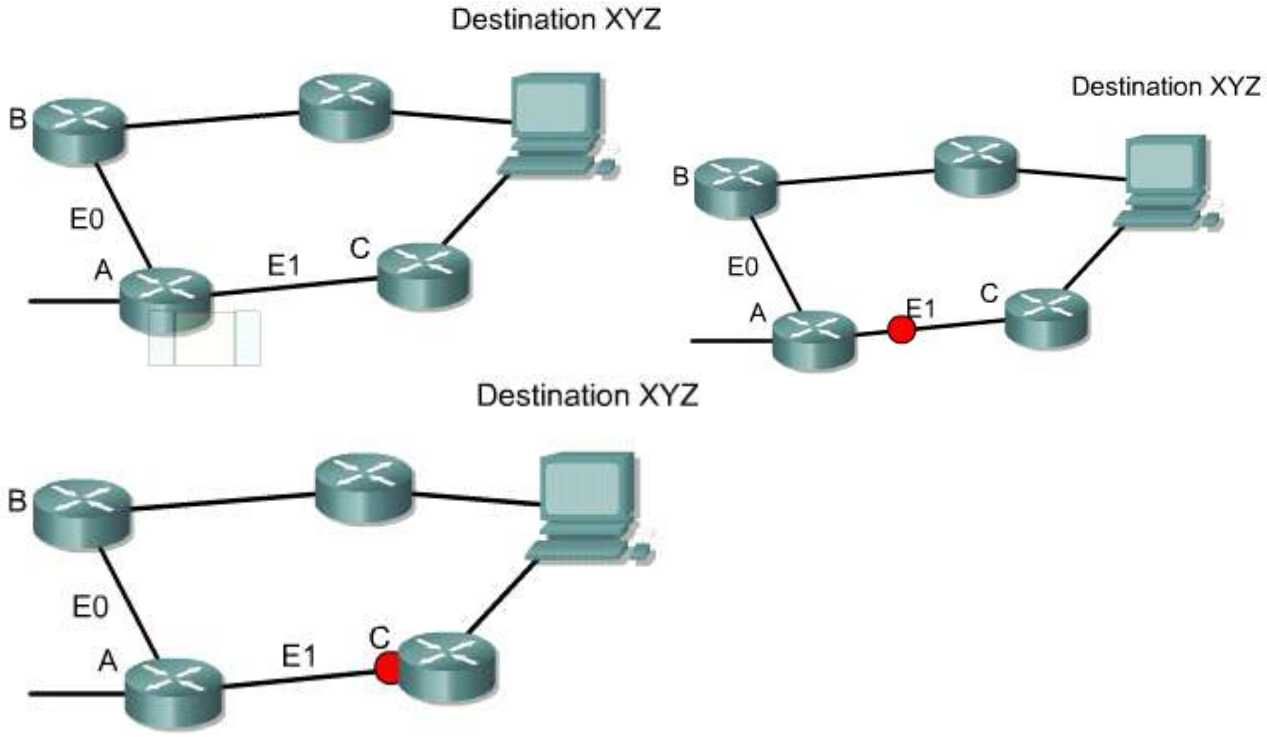
Destination XYZ



Destination XYZ

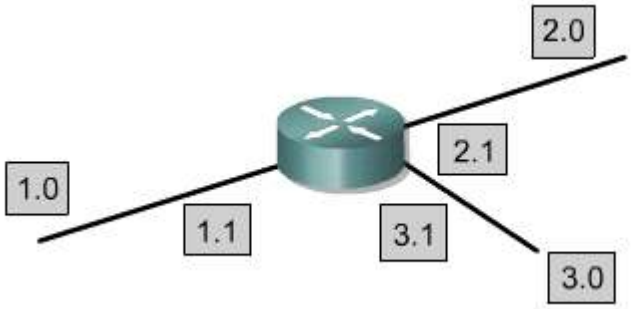






La fonction de commutation est le processus interne qu'utilise un routeur pour accepter un paquet sur une interface et le transmettre à une deuxième interface sur le même routeur. La fonction de commutation a pour responsabilité principale d'encapsuler les paquets dans le type de trame approprié pour la prochaine liaison.

La figure 5 illustre la façon dont les routeurs utilisent l'adressage pour exécuter les fonctions de routage et de commutation. Le routeur utilise la portion réseau de l'adresse pour sélectionner le chemin qui permettra de transmettre le paquet au prochain routeur situé sur le chemin.



Réseau de destination	Port de routeur et direct
1.0	1.1
2.0	2.1
3.0	3.1
• La portion réseau de l'adresse sert à sélectionner le chemin. • La portion nœud de l'adresse indique le port du routeur pour le chemin.	

6.3 Vue d'ensemble des protocoles de routage

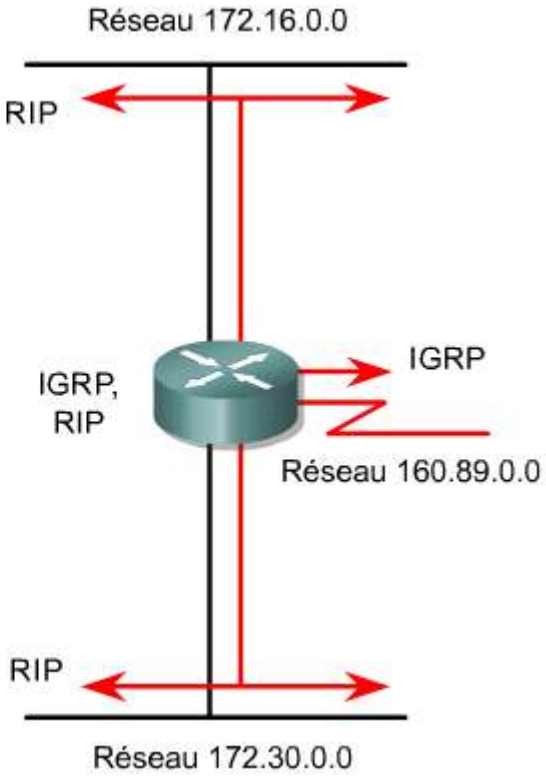
6.3.2 Configuration de routage

L'activation d'un protocole de routage IP implique la définition de paramètres généraux et de paramètres de routage. Les tâches globales comprennent la sélection d'un protocole de routage, tel que RIP, IGRP, EIGRP ou OSPF. Les principales tâches dans le mode de configuration consistent à indiquer les numéros de réseau IP. Le routage dynamique utilise des

messages de diffusion broadcast et multicast pour communiquer avec les autres routeurs. La métrique de routage aide les routeurs à trouver le meilleur chemin menant à chaque réseau ou sous-réseau. 1

Configuration globale
Sélection du ou des protocoles de routage Indication du ou des réseaux

Configuration de l'interface
Vérification du masque d'adresse/de sous-réseau



La commande **router** lance le processus de routage. 2 3

Commande

```
Router(config)#router protocol [options]
```

Défini un protocole de routage.

Commande

```
Router(config-router)#network network-number
```

La sous-commande **network** est obligatoire pour chaque protocole de routage utilisé.

Commande router	Description
protocole	IGRP, EIGRP, OSPF ou RIP
options	IGRP et EIGRP nécessitent un numéro de système autonome. OSPF nécessite une identification de procédé. RIP na besoin daucun de ces paramètres.

La commande **network** est nécessaire, car elle permet au processus de routage de déterminer les interfaces qui participeront à l'envoi et à la réception des mises à jour du routage. 2 4

Commande network	Description
network number	Définit un réseau directement connecté.

Voici un exemple de configuration de routage:

```
GAD(config)#router rip
GAD(config-router)#network 172.16.0.0
```

Les numéros de réseau sont basés sur les adresses de classe, et non sur les adresses de sous-réseau ou des adresses hôtes. Les principales adresses réseau se limitent aux numéros de réseau des classes A, B et C.

Activité de TP

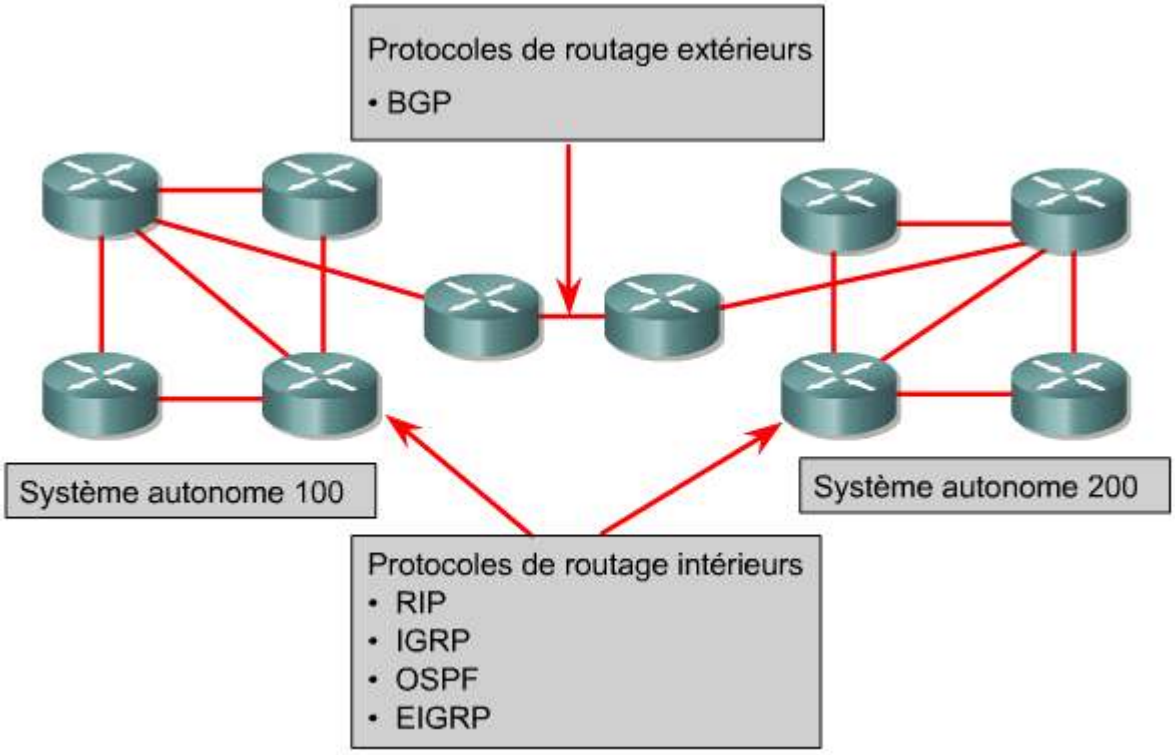
Activité en ligne : Configuration du routage

Au cours de ce TP, les étudiants vont configurer les routeurs pour démarrer un processus de routage, puis ajouter les réseaux qui seront annoncés.

6.3 Vue d'ensemble des protocoles de routage

6.3.3 Protocoles de routage

Au niveau de la couche Internet de l'ensemble de protocoles de la pile TCP/IP, un routeur peut utiliser un protocole de routage IP pour réaliser le routage par la mise en oeuvre d'un algorithme de routage particulier. Les protocoles suivants sont des exemples de protocoles de routage IP: 1



- **RIP** – Protocole de routage interne à vecteur de distance.
- **IGRP** – Protocole de routage interne à vecteur de distance de Cisco.
- **OSPF** – Protocole de routage intérieur à état de liens
- **EIGRP** – Protocole de routage intérieur à vecteur de distance avancé de Cisco.
- **BGP** – Protocole de routage extérieur à vecteur de distance

Le protocole RIP a été initialement défini dans la RFC 1058. Ses principales caractéristiques sont les suivantes:

- Il s'agit d'un protocole de routage à vecteur de distance.
- Il utilise le nombre de sauts comme métrique pour la sélection du chemin.
- Si le nombre de sauts est supérieur à 15, le paquet est éliminé.
- Par défaut, les mises à jour du routage sont diffusées toutes les 30 secondes.

Le protocole IGRP (Interior Gateway Routing Protocol) est un protocole propriétaire développée par Cisco. De par sa conception, le protocole IGRP est doté, entre autres, des caractéristiques suivantes:

- Il s'agit d'un protocole de routage à vecteur de distance.
- La bande passante, la charge, le délai et la fiabilité sont utilisés pour créer une métrique composite.
- Par défaut, les mises à jour du routage sont diffusées toutes les 90 secondes.

Le protocole OSPF (Open Shortest Path First) est un protocole de routage à état de liens non propriétaire. Les caractéristiques clés de ce protocole sont les suivantes:

- Il s'agit d'un protocole de routage à état de liens.
- C'est un protocole de routage de norme ouverte décrit dans les requêtes pour commentaires RFC 2328.
- Il utilise l'algorithme SPF pour calculer le coût le plus bas vers une destination.
- Les mises à jour du routage sont diffusées à mesure des modifications de topologie.

Le protocole EIGRP est un protocole de routage à vecteur de distance amélioré et propriétaire développé par Cisco. Les caractéristiques clés de ce protocole sont les suivantes:

- Il s'agit d'un protocole de routage à vecteur de distance amélioré.
- Il utilise l'équilibrage de charge en coût différencié.
- Il utilise une combinaison de fonctions à vecteur de distance et à état de liens.
- Il utilise l'algorithme DUAL (Diffusing Update Algorithm) pour calculer le chemin le plus court.
- Les mises à jour du routage sont diffusées en mode multicast en utilisant l'adresse 224.0.0.10 et sont déclenchées par des modifications topologiques.

Le protocole BGP (Border Gateway Protocol) est un protocole de routage extérieur. Les caractéristiques clés de ce protocole sont les suivantes:

- Il s'agit d'un protocole de routage extérieur à vecteur de distance.
- Il est utilisé pour la connexion entre les FAI ou entre les FAI et les clients.
- Il est utilisé pour acheminer le trafic Internet entre des systèmes autonomes.

Activité de média interactive

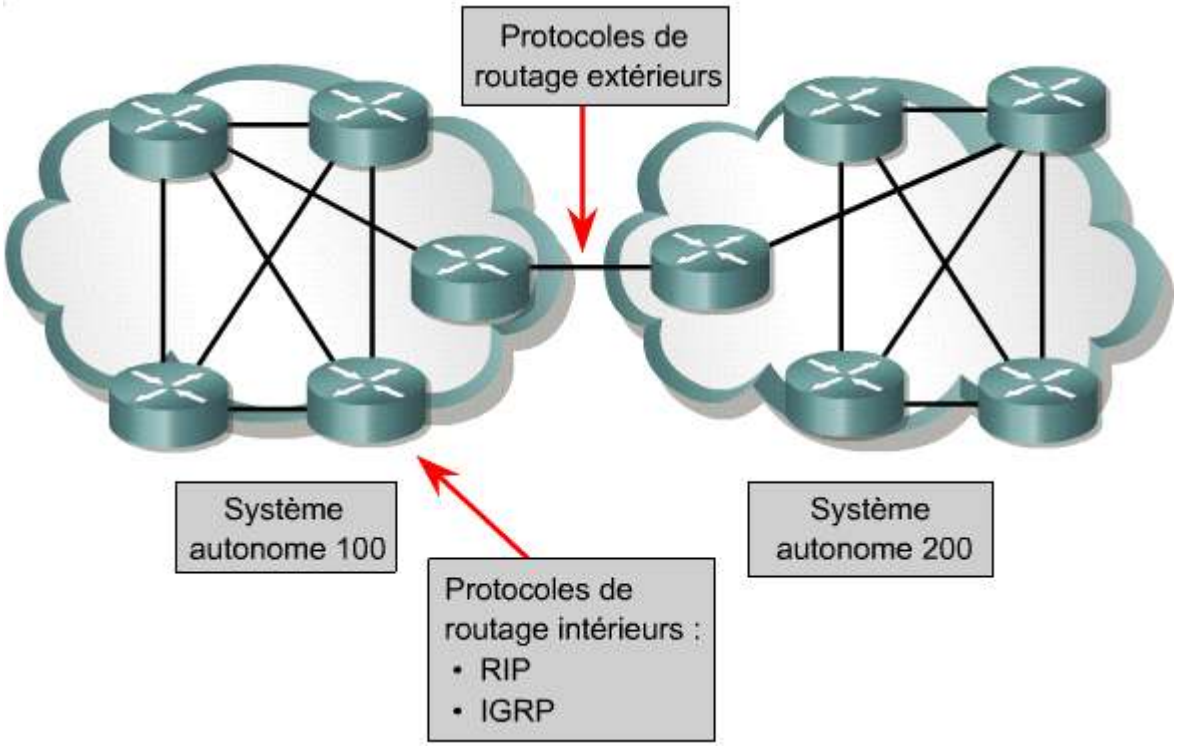
Case à cocher : Protocoles de routage à état de liens et à vecteur de distance

À la fin de cette activité, l'étudiant sera en mesure de comprendre les protocoles de routage IP.

6.3 Vue d'ensemble des protocoles de routage

6.3.4 Systèmes autonomes et comparatif IGP - EGP

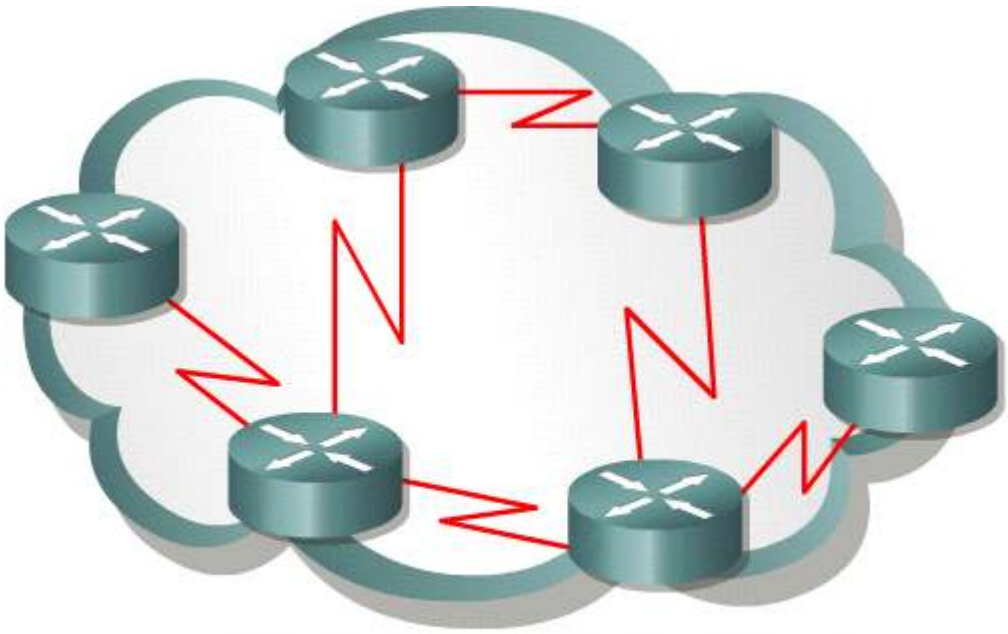
Les protocoles de routage intérieurs sont destinés à être utilisés dans un réseau dont les différentes parties sont sous le contrôle d'une organisation unique. Les critères de conception d'un protocole de routage intérieur requièrent que celui-ci trouve le meilleur chemin possible sur le réseau. Autrement dit, la métrique et la façon dont cette métrique est utilisée est l'élément le plus important d'un protocole de routage intérieur. 1



Ce protocole de routage est conçu pour une utilisation entre deux réseaux différents qui sont sous le contrôle de deux organisations différentes. En règle générale ils sont utilisés pour la communication entre les fournisseurs d'accès ou entre une société et un FAI. Par exemple, une société pourra exécuter le BGP, un protocole de routage extérieur, entre l'un de ses routeurs et un routeur installé chez un FAI. Les protocoles de passerelle extérieurs IP nécessitent les trois ensembles d'informations suivants pour que le routage puisse commencer:

- Une liste des routeurs voisins avec lesquels échanger des informations de routage.
- Une liste de réseaux à annoncer comme étant directement accessibles.
- Le numéro du système autonome du routeur local.

Un protocole de routage extérieur doit isoler les systèmes autonomes. Souvenez-vous que les systèmes autonomes sont gérés par différentes administrations. Les réseaux doivent disposer d'un protocole pour communiquer entre ces différents systèmes.
2



Routeurs sous administration commune

Les systèmes autonomes possèdent un numéro d'identification qui leur est attribué par l'InterNIC (Internet Network Information Center) ou par un fournisseur de services. Ce numéro est un nombre à 16 bits. Les protocoles de routage, tels que l'IGRP et l'EIGRP de Cisco, nécessitent l'attribution d'un numéro de système autonome unique.

Activité de média interactive

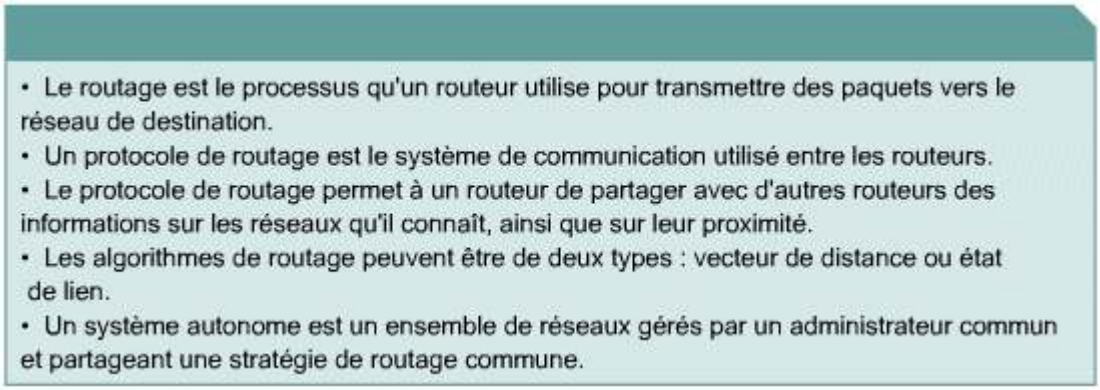
Case à cocher : IGP et EGP

À la fin de cette activité, l'étudiant sera en mesure de comprendre les protocoles IGP et EGP.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Un routeur ne peut transmettre un paquet sans connaître de route vers un réseau de destination
- Les administrateurs réseau configurent les routes statiques manuellement
- Les routes par défaut sont des routes statiques spéciales qui fournissent aux routeurs des passerelles de dernier recours
- Les routes statiques et par défaut sont configurées à l'aide de la commande **`ip route`**
- La configuration d'une route statique ou d'une route par défaut peut être vérifiée à l'aide des commandes **`show ip route`**, **`ping`** et **`traceroute`**
- Vérification et dépannage des routes statiques et des routes par défaut
- Protocoles de routage
- Systèmes autonomes
- Objet des protocoles de routage et des systèmes autonomes
- Classes de protocoles de routage
- Fonctions du protocole de routage à vecteur de distance et exemples
- Fonctions et exemples de protocole à état de liens
- Détermination de route
- Configuration de routage
- Protocoles de routage (RIP, IGRP, OSPF, EIGRP, BGP)
- Systèmes autonomes et comparatif des protocoles IGP et EGP
- Routage à vecteur de distance
- Routage à état de liens.



Vue d'ensemble

Les protocoles de routage dynamique peuvent simplifier le travail d'un administrateur réseau. Le routage dynamique permet d'éviter le processus fastidieux et astreignant de configuration de routes statiques. Par ailleurs, grâce au routage dynamique, les routeurs peuvent réagir aux changements survenus sur le réseau et modifier leurs tables de routage en conséquence, sans intervention de la part de l'administrateur réseau. Toutefois, le routage dynamique peut causer des problèmes. Certains des problèmes associés aux protocoles de routage dynamique à vecteur de distance, ainsi que les solutions développées par les concepteurs de ces protocoles, sont traités dans ce module.

RIP (Routing Information Protocol) est un protocole de routage à vecteur de distance utilisé sur des milliers de réseaux à travers le monde. Parce qu'il est basé sur des normes ouvertes et qu'il est très simple à mettre en œuvre, ce protocole est particulièrement intéressant pour certains administrateurs réseau, bien qu'il ne dispose pas de la puissance et des

fonctionnalités des protocoles de routage plus évolués. De par sa simplicité, le protocole RIP représente un bon point de départ pour les étudiants en technologie réseau. Ce module présente également les procédures de configuration et de dépannage du protocole RIP.

À l'instar du protocole RIP, IGRP (Interior Gateway Routing Protocol) est un protocole de routage à vecteur de distance. En revanche, à la différence du protocole RIP, IGRP est un protocole propriétaire de Cisco, et non un protocole basé sur des normes ouvertes. Bien qu'il reste simple à mettre en œuvre, il est plus complexe que RIP et il peut utiliser un certain nombre de facteurs pour déterminer le meilleur chemin vers un réseau de destination. Ce module présente également les procédures de configuration et de dépannage du protocole IGRP.

À la fin de ce module, les étudiants doivent être en mesure de:

- Comprendre les raisons de l'apparition de boucles de routage dans le cadre du routage à vecteur de distance
- Décrire les différentes méthodes utilisées par les protocoles de routage à vecteur de distance afin de garantir l'exactitude des informations de routage
- Configurer le protocole RIP
- Utiliser la commande **`ip classless`**
- Résoudre les problèmes associés au protocole RIP
- Configurer RIP pour l'équilibrage de charge
- Configurer des routes statiques pour RIP
- Vérifier la configuration RIP
- Configurer le protocole IGRP
- Vérifier le fonctionnement du protocole IGRP
- Résoudre les problèmes associés au protocole IGRP

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
7.1	Routage à vecteur de distance
7.2	RIP
7.3	IGRP

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Sélection d'un protocole de routage approprié d'après les besoins des utilisateurs	• Configuration de protocoles de routage d'après les besoins des utilisateurs	• Dépannage de protocoles de routage	• Évaluation des caractéristiques des protocoles de routage

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Sélection d'un protocole de routage approprié d'après les besoins des utilisateurs	• Configuration de protocoles de routage d'après les besoins des utilisateurs • Mise en œuvre d'un LAN	• Dépannage de protocoles de routage	• Évaluation des caractéristiques des protocoles de routage

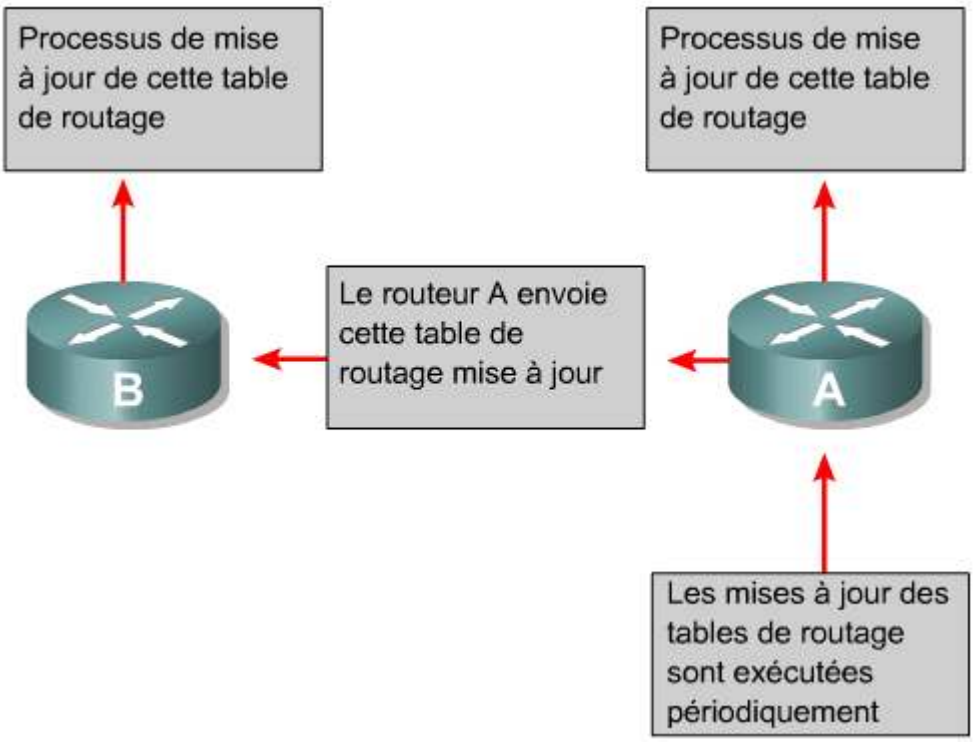
Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
		• Description des concepts associés au routage, ainsi que des différents protocole et méthodes visant à sa réalisation

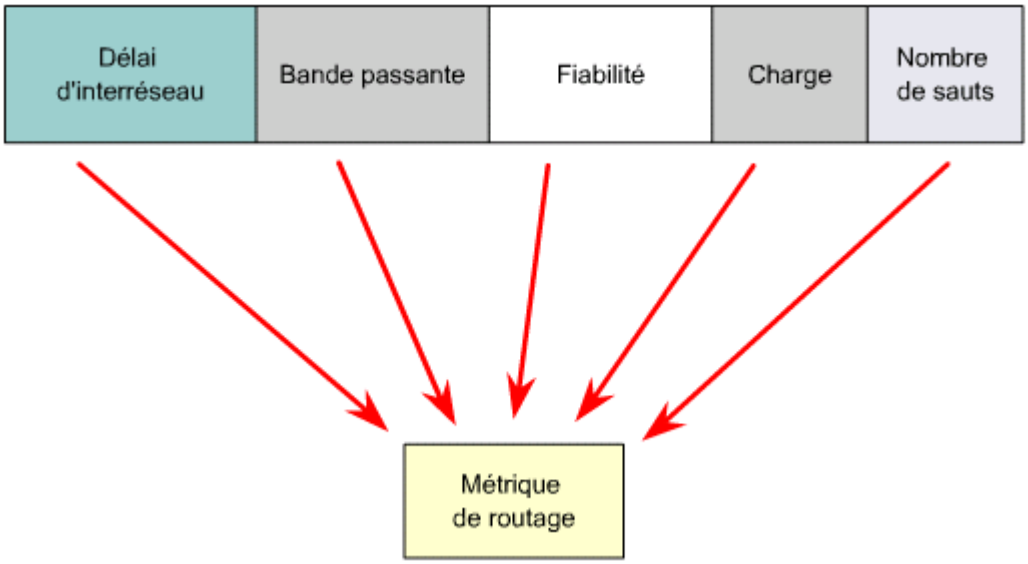
7.1 Routage à vecteur de distance

7.1.1 Mises à jour du routage à vecteur de distance

Les tables de routage sont mises à jour périodiquement ou lorsque la topologie d'un réseau basé sur un protocole à vecteur de distance change. Il est important qu'un protocole de routage puisse mettre à jour de façon efficace les tables de routage. Comme dans le cas du processus de découverte de réseau, la mise à jour des modifications topologiques s'effectue systématiquement d'un routeur à l'autre. 1



Les algorithmes à vecteur de distance prévoient que chaque routeur transmette aux routeurs voisins l'intégralité de sa table de routage. Les tables de routage contiennent des informations sur le coût total du chemin (défini par la métrique) et l'adresse logique du premier routeur sur le chemin menant à chaque réseau contenu dans la table. 2

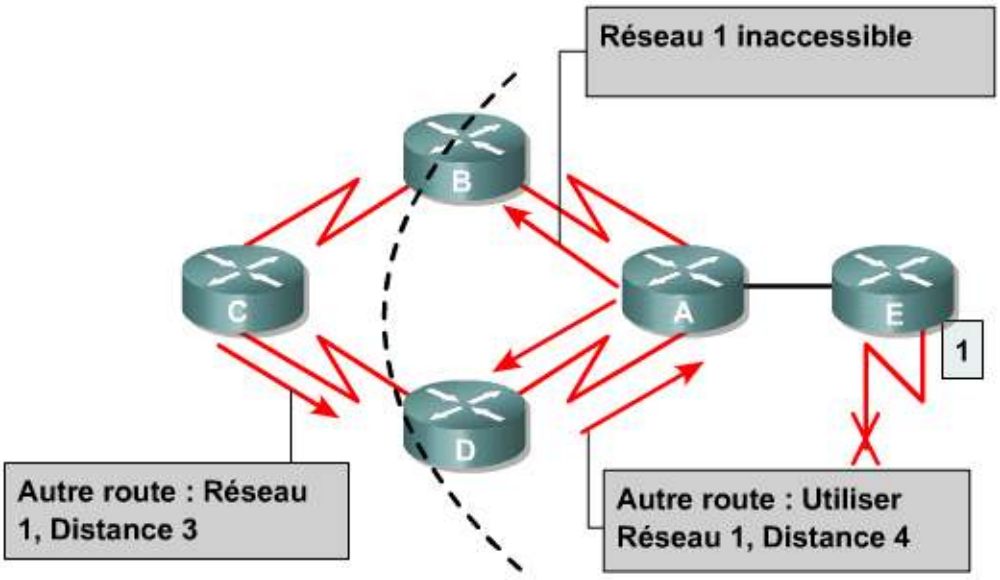


7.1 Routage à vecteur de distance

7.1.2 Problèmes liés aux boucles de routage à vecteur de distance

Des boucles de routage peuvent apparaître lorsque des tables de routage incohérentes ne sont pas mises à jour en raison d'une convergence plus lente dans un environnement réseau changeant. 1

1. Juste avant la panne du réseau 1, tous les routeurs disposent d'une base de connaissances cohérente et de tables de routage correctes. On dit alors que le réseau a convergé. Pour la suite de cet exemple, supposons que le meilleur chemin du routeur C vers le réseau 1 passe par le routeur B et que la distance entre le routeur C et le réseau 1 soit égale à 3.
2. Lorsque le réseau 1 tombe en panne, le routeur E envoie une mise à jour au routeur A. Ce dernier cesse d'acheminer des paquets vers le réseau 1, mais les routeurs B, C et D continuent de les acheminer car ils n'ont pas encore été informés de la panne. Lorsque le routeur A transmet sa mise à jour, les routeurs B et D cessent d'acheminer des paquets vers le réseau 1. Toutefois, le routeur C n'a toujours pas reçu de mise à jour. Pour lui, le réseau 1 est toujours accessible via le routeur B.
3. À présent, le routeur C envoie une mise à jour périodique au routeur D pour lui indiquer un chemin vers le réseau 1 passant par le routeur B. Le routeur D modifie sa table de routage pour refléter cette information erronée et la transmet au routeur A. Ce dernier la transmet à son tour aux routeurs B et E, et ainsi de suite. Tous les paquets destinés au réseau 1 génèrent alors une boucle à partir du routeur C vers les routeurs B, A et D, qui revient au routeur C.

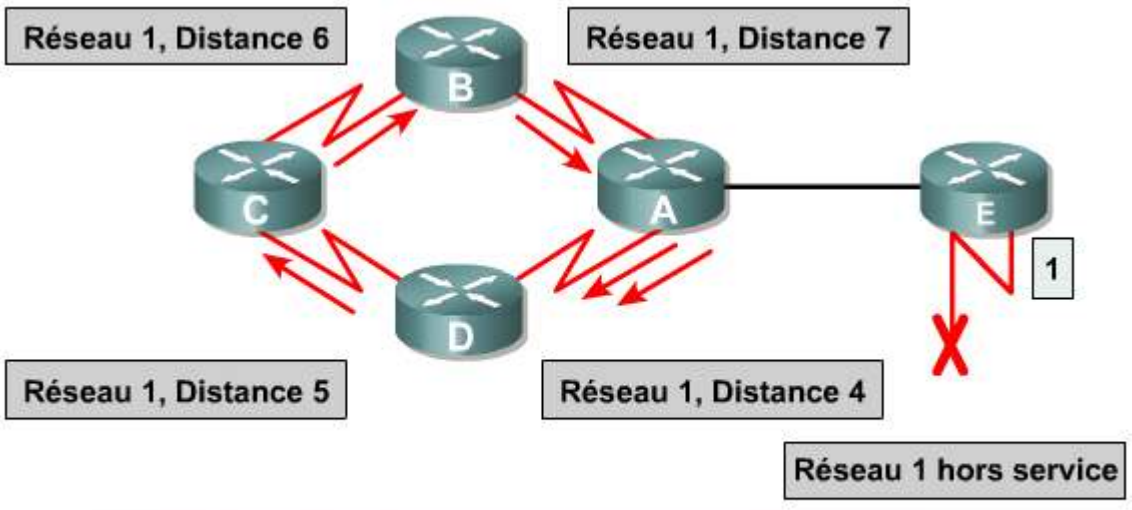


Autres routes, convergence lente, routage incohérent

7.1 Routage à vecteur de distance

7.1.3 Définition d'une valeur maximale

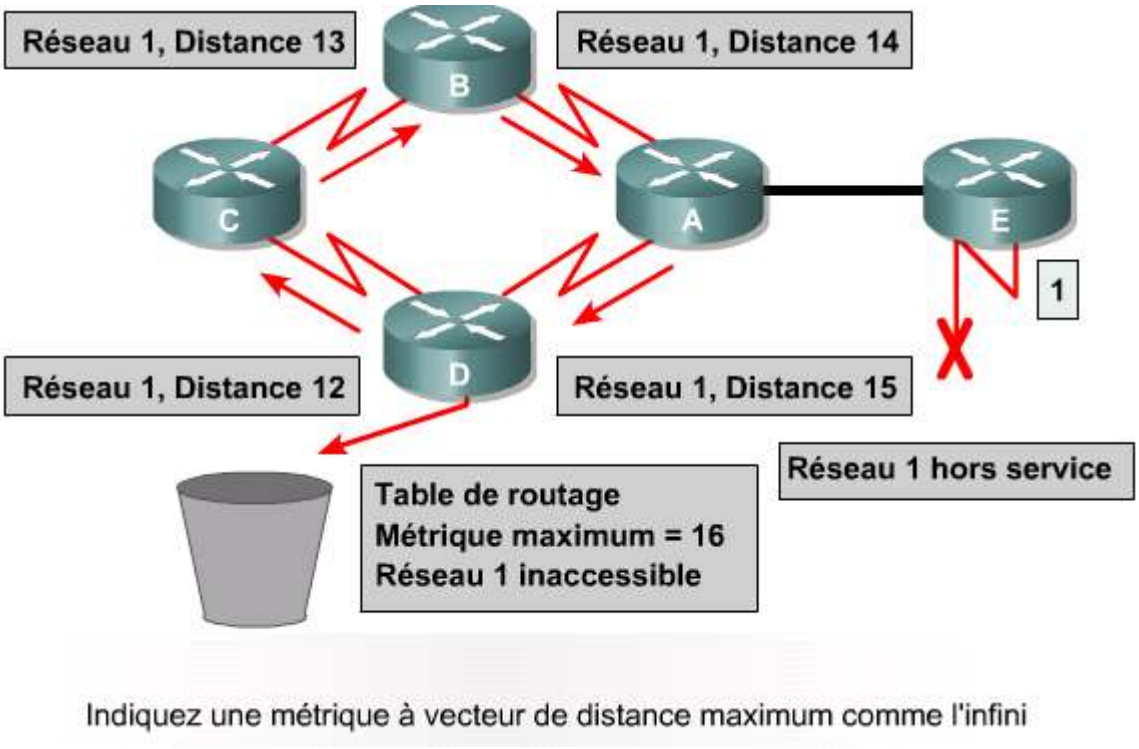
Les mises à jour erronées du réseau 1 continueront de former une boucle jusqu'à ce qu'un autre processus mette fin au bouclage. En raison de cette condition, appelée métrique de mesure infinie, les paquets tournent sans cesse sur une boucle bien que le réseau de destination (réseau 1) soit en panne. Tandis que les routeurs comptent à l'infini, les informations erronées permettent l'existence d'une boucle de routage. [1]



Boucles de routage incrémentant le vecteur de distance

Si aucune mesure n'est prise pour arrêter ce processus, la métrique à vecteur de distance du nombre de sauts est incrémentée chaque fois que le paquet passe par un autre routeur. Les paquets tournent en boucle sur le réseau en raison de la présence d'informations erronées dans les tables de routage.

Les algorithmes de routage à vecteur de distance sont autocorrectifs. Toutefois, pour régler un problème de boucle de routage, une métrique de mesure infinie peut s'avérer nécessaire. Pour éviter que le problème se prolonge, les protocoles à vecteur de distance définissent l'infini en tant que nombre maximal spécifique. Ce nombre fait référence à une métrique de routage qui peut simplement correspondre au nombre de sauts. [2]



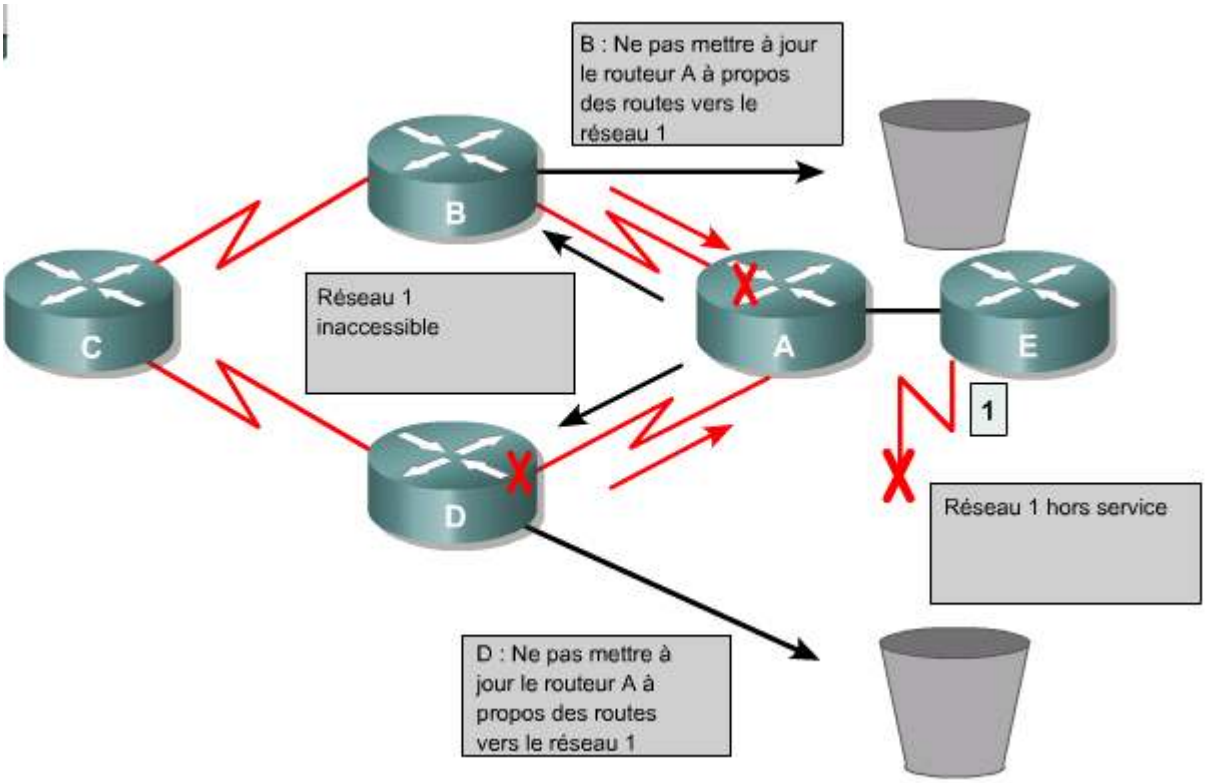
Grâce à cette méthode, le protocole de routage permet à la boucle de routage d'exister jusqu'à ce que la métrique dépasse la valeur maximale autorisée. Le graphique indique une valeur métrique de 16 sauts qui dépasse la valeur maximale par défaut du vecteur de distance égale à 15 sauts. Le routeur ignore donc le paquet. Dans tous les cas, le réseau 1 est considéré comme inaccessible lorsque la valeur métrique dépasse la valeur maximale.

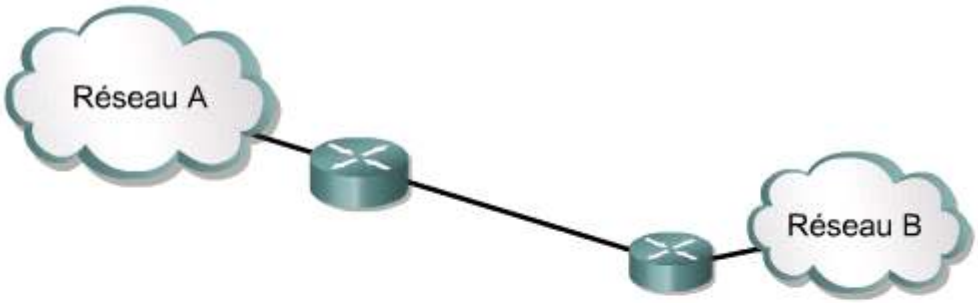
7.1 Routage à vecteur de distance

7.1.4 Élimination des boucles de routage grâce à la fonction split horizon

Une boucle de routage peut également se créer lorsqu'un routeur reçoit des informations erronées qui contredisent les informations correctes qu'il a envoyées initialement. Ce problème survient de la façon suivante:

1. Le routeur A transmet une mise à jour aux routeurs B et D indiquant que le réseau 1 est arrêté. Cependant, le routeur C transmet une mise à jour au routeur B indiquant que le réseau 1 est disponible à une distance de 4, via le routeur D. Ce chemin ne transgresse pas les règles de la solution split horizon.
2. Le routeur B en conclut, à tort, que le routeur C dispose toujours d'un chemin valide vers le réseau 1, bien que la métrique soit beaucoup moins favorable. Le routeur B transmet une mise à jour au routeur A pour lui indiquer la nouvelle route jusqu'au réseau 1.
3. Le routeur A détermine maintenant qu'il peut envoyer des paquets au réseau 1 via le routeur B. Ce dernier détermine qu'il peut les envoyer au réseau 1 via le routeur C, et celui-ci détermine qu'il peut les envoyer au réseau 1 via le routeur D. Tous les paquets introduits dans cet environnement tourneront en boucle entre les routeurs.
4. La solution split horizon tente d'éviter cette situation. Si une mise à jour de routage relative au réseau 1 arrive du routeur A, le routeur B ou D n'est pas en mesure de renvoyer au routeur A les informations relatives au réseau 1. La solution split horizon réduit ainsi les informations de routage erronées, ainsi que la charge de routage.

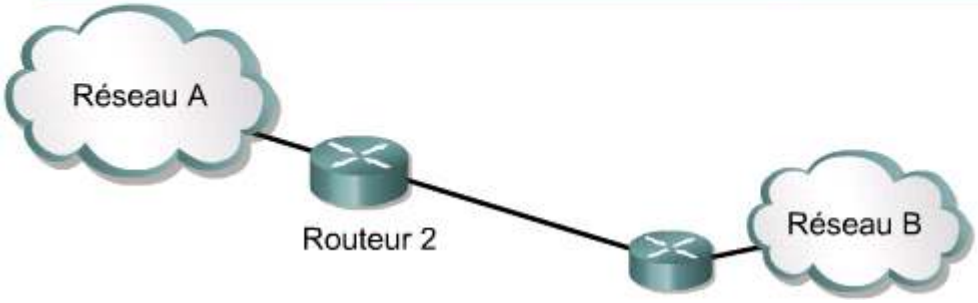




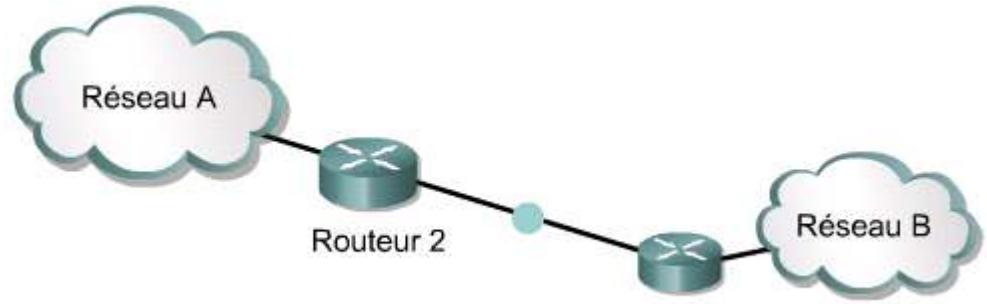
Popup Window

En " split-horizon " simple, les mises à jour de routage envoyées par un routeur à son voisin ne contiennent pas les informations qui ont été précédemment apprises grâce à ce routeur voisin. Supposons, par exemple, que le routeur 1 annonce qu'il connaît une route vers le réseau A. Le routeur 2 reçoit la mise à jour du routeur 1 et insère cette information sur le réseau A dans sa table de routage. Lors des mises à jour régulières des informations de routage envoyées au routeur 1, le routeur 2 n'inclura pas l'entrée concernant le réseau A, puisque c'est ce routeur 1 qui lui avait indiqué une route vers ce réseau A.

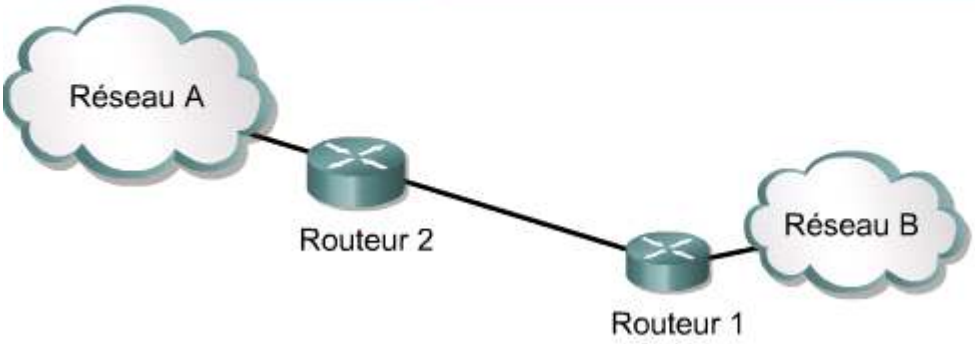
Dest.	Métrique	Saut suiv.
A	0	n/a



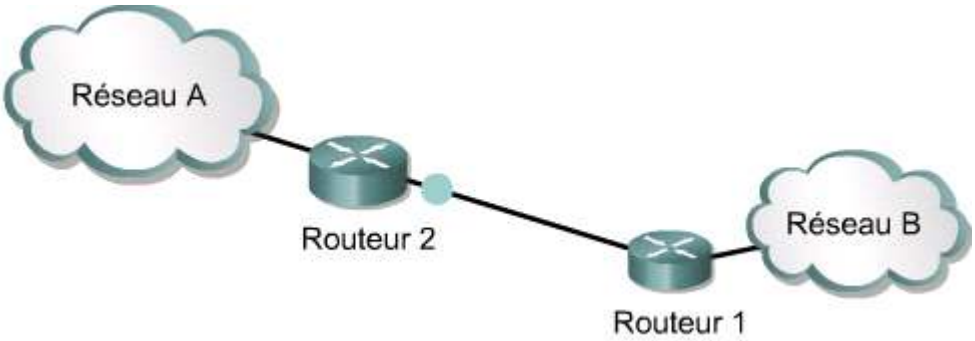
R2 ⟶ R1



Dest.	Métrique	Saut suiv.
A	0	n/a
B	0	n/a



R1 ⟶ R2



7.1 Routage à vecteur de distance

7.1.5 Mode poison reverse

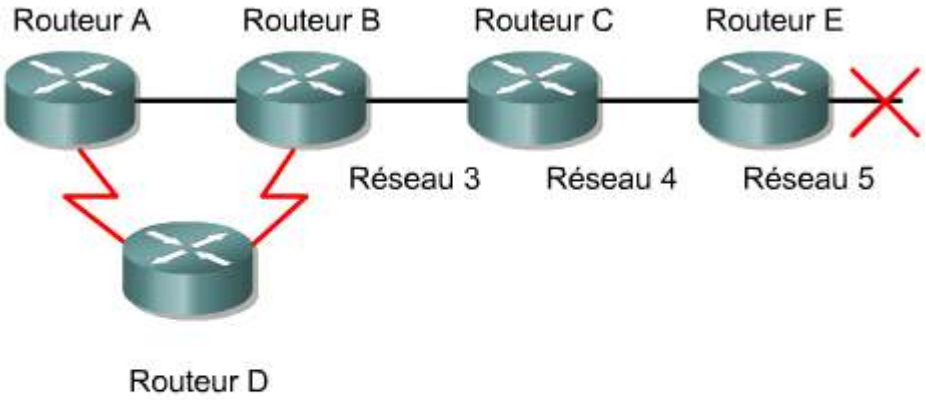
Le mode « poison reverse » est utilisé par différents protocoles à vecteur de distance afin d'éviter les grandes boucles de routage et d'offrir des informations explicites en cas d'inaccessibilité d'un sous-réseau ou d'un réseau. En règle générale, ce mode ajoute 1 au nombre maximal de sauts.

Le mode poison reverse constitue l'un des moyens d'éviter les mises à jour incohérentes. Lorsque le réseau 5 tombe en panne, le routeur E passe en mode poison reverse en créant une entrée de table de métrique 16 (inaccessible) pour ce réseau. 1 De cette manière, le routeur C n'est plus susceptible de transmettre des mises à jour incorrectes concernant la route vers le réseau 5. Lorsqu'il reçoit un message poison reverse en provenance du routeur E, il renvoie à ce dernier une mise à jour poison reverse. Cela permet de s'assurer que toutes les routes du segment ont bien reçu les informations sur la route inaccessible.

Grâce au mode poison reverse et aux mises à jour déclenchées, le temps de convergence est plus rapide car les routeurs voisins n'ont pas à attendre 30 secondes avant d'annoncer la route inaccessible.

En mode poison reverse, un protocole de routage annonce les routes inaccessibles avec une métrique de mesure infinie. Ce mode n'est pas contraire aux règles split horizon. La méthode split horizon avec poison reverse consiste essentiellement à empêcher l'utilisation d'une route, mais elle concerne plus particulièrement les routes que les règles split horizon

n'autoriseraient pas normalement pour la transmission des informations de routage. Dans chacun des cas, les routes inaccessibles sont annoncées avec des métriques de mesure infinie.



Lorsque le réseau 5 tombe en panne, le routeur E passe en mode " poison reverse " en créant une entrée de table de métrique 16 (inaccessible)

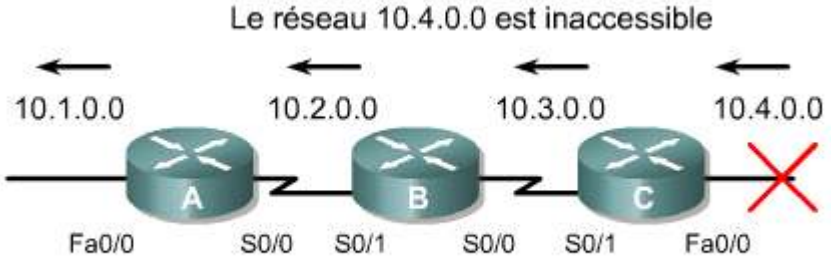
7.1 Routage à vecteur de distance

7.1.6 Comment empêcher les boucles de routage avec les mises à jour déclenchées

Les nouvelles tables de routage sont envoyées régulièrement aux routeurs voisins. Par exemple, les mises à jour RIP ont lieu toutes les 30 secondes. Toutefois, une mise à jour déclenchée est envoyée immédiatement en réponse à certaines modifications de la table de routage. Le routeur qui détecte une modification topologique envoie immédiatement un message de mise à jour aux routeurs adjacents qui, à leur tour, génèrent des mises à jour déclenchées pour signaler la modification à leurs routeurs voisins. En cas d'échec d'une route, une mise à jour est envoyée immédiatement, sans attendre l'expiration du délai du compteur de mise à jour. Les mises à jour déclenchées, associées à la fonction poison reverse, permettent de s'assurer que tous les routeurs ont connaissance des routes inaccessibles avant l'expiration du délai des compteurs de retenue.

Les mises à jour déclenchées continuent à envoyer des mises à jour en raison d'un changement des informations de routage, sans attendre l'expiration du délai du compteur. Le routeur envoie une autre mise à jour de routage sur ses autres interfaces, sans attendre l'expiration du délai du compteur de mise à jour de routage. Cela entraîne la transmission des informations relatives à l'état de la route qui a changé et le déclenchement plus rapide des compteurs de retenue sur les routeurs voisins. La vague de mises à jour se propage sur l'ensemble du réseau.

Le routeur C déclenche une mise à jour pour annoncer que le réseau 10.4.0.0 est inaccessible. 1 Lorsqu'il reçoit cette information, le routeur B annonce l'indisponibilité de ce réseau via l'interface S0/1. Le routeur A envoie à son tour une mise à jour à partir de l'interface Fa0/0.



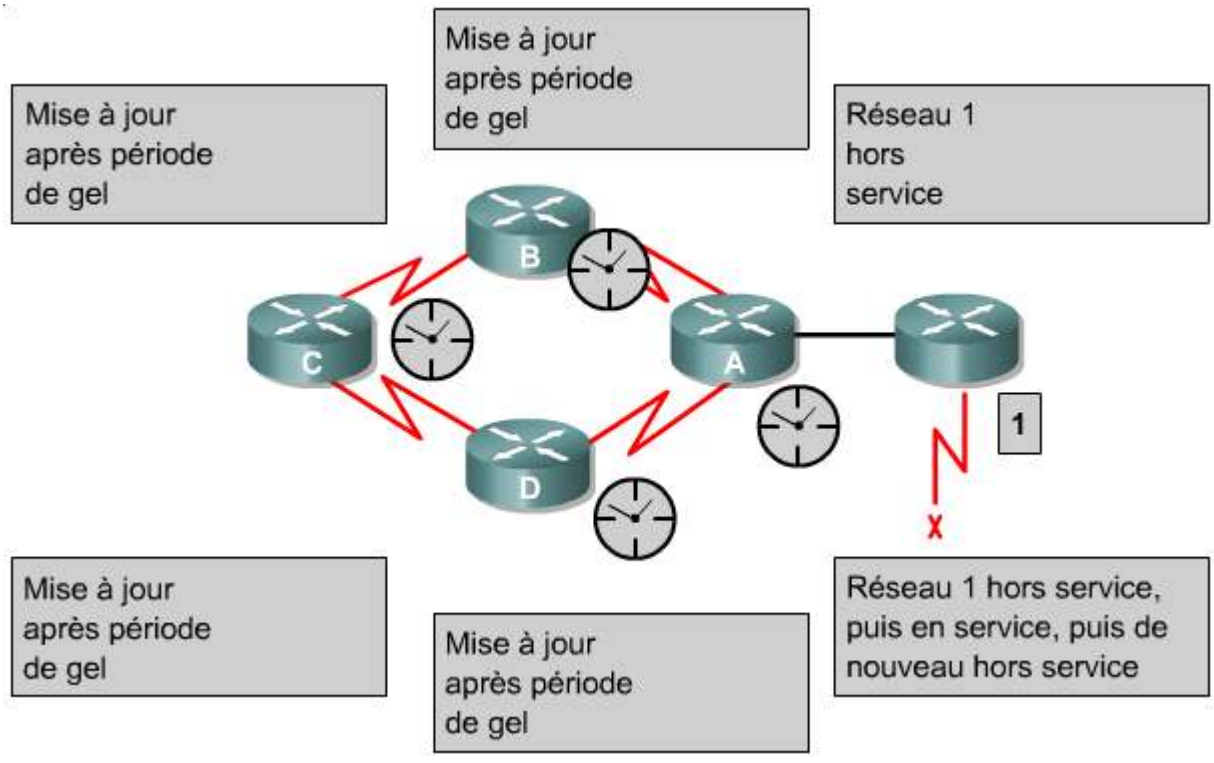
Avec le concept de mise à jour déclenchée, les routeurs envoient des messages dès qu'ils remarquent un changement dans leur table de routage.

7.1 Routage à vecteur de distance

7.1.7 Comment éviter les boucles de routage grâce aux compteurs de retenue

L'utilisation de compteurs de retenue permet d'éviter les problèmes de métrique de mesure infinie: 1

- Lorsqu'un routeur reçoit une mise à jour d'un routeur voisin lui indiquant qu'un réseau auparavant accessible est devenu inaccessible, il marque la route comme étant inaccessible et déclenche un compteur de retenue. Si, avant l'expiration du délai de retenue, le routeur reçoit une mise à jour du même voisin indiquant que le réseau est de nouveau accessible, il marque le réseau comme étant accessible et désactive le compteur de retenue.
- Si une mise à jour provenant d'un autre routeur voisin indique une métrique meilleure que celle initialement enregistrée pour le réseau, le routeur marque le réseau comme étant accessible et désactive le compteur de retenue.
- Si, avant l'expiration du délai de retenue, une mise à jour provenant d'un autre routeur voisin indique une métrique inférieure, elle est ignorée. Le fait d'ignorer une telle mise à jour alors qu'un compteur de retenue est actif permet de disposer de plus de temps pour transmettre à l'ensemble du réseau les informations relatives à une modification perturbatrice.



7.2 RIP

7.2.1 Processus de routage RIP

a version moderne, standard et ouverte de RIP, quelquefois appelée IP RIP, est décrite officiellement dans deux documents distincts. Le premier s'intitule Requête pour commentaires (Request for Comments - RFC) 1058 et l'autre Norme Internet (Internet Standard – STD) 56. 1

Le protocole RIP a évolué au fil des années pour passer d'un protocole de routage par classes, RIP Version 1 (RIP v1), à un protocole de routage sans classe, RIP Version 2 (RIP v2). La version RIP v2 présente les améliorations suivantes:

- Possibilité de transmettre des informations supplémentaires sur le routage de paquets.
- Mécanisme d'authentification visant à sécuriser la mise à jour de tables.
- Prise en charge des masques de sous-réseau de longueur variable (VLSM).

Le protocole RIP permet d'empêcher les boucles de routage infinies grâce à la définition d'un nombre maximum de sauts autorisé sur un chemin entre la source et une destination. Le nombre maximum de sauts sur un chemin est 15. Lorsqu'un routeur reçoit une mise à jour de routage contenant une nouvelle entrée ou une entrée modifiée, la valeur métrique augmente de 1 et représente un saut sur le chemin. Si la métrique dépasse alors 15, on considère que cela correspond à l'infini et que le réseau de destination est inaccessible. Le protocole RIP comporte des fonctions communes à d'autres protocoles de routage comme les mécanismes split horizon et de gel permettant d'empêcher la propagation des informations de routage incorrectes.

Les principales caractéristiques du protocole RIP sont les suivantes :

- Il s'agit d'un protocole de routage à vecteur de distance.
- Le nombre de sauts est la métrique utilisée pour sélectionner le chemin.
- Si le nombre de sauts est supérieur à 15, le paquet est éliminé.
- Par défaut, les mises à jour du routage sont diffusées toutes les 30 secondes.

7.2 RIP

7.2.2 Configuration du protocole RIP

La commande **`router rip`** permet de sélectionner le protocole RIP comme protocole de routage. La commande **`network`** permet d'indiquer au routeur les interfaces sur lesquelles exécuter RIP. Le processus de routage associe les interfaces spécifiques aux adresses réseau, puis commence à envoyer et à recevoir les mises à jour RIP sur ces interfaces.

Le protocole RIP envoie des messages de mise à jour de routage à intervalles réguliers. Lorsqu'un routeur reçoit une mise à jour de routage avec modification d'une entrée, il met à jour sa table de routage en conséquence. La valeur métrique reçue pour le chemin est incrémentée de 1 et l'interface source de la mise à jour apparaît comme saut suivant dans la table de routage. Les routeurs RIP conservent uniquement la meilleure route vers une destination mais ils peuvent également gérer plusieurs chemins de coût égal vers une destination.

La plupart des protocoles de routage utilisent une combinaison de mises à jour soit périodiques, soit déclenchées par des changements sur le réseau. RIP utilise des mises à jour périodiques, mais la mise en œuvre de RIP par Cisco envoie des mises à jour dès qu'un changement dans la topologie est détecté. Les changements dans la topologie déclenchent aussi des mises à jour immédiates sur les routeurs IGRP, quelque soit l'état des compteurs périodiques. Sans ces mises à jour, RIP et IGRP ne fonctionneraient pas de façon satisfaisante. Après avoir mis à jour sa table de routage en accord avec la modification de la configuration, le routeur commence à transmettre des mises à jour de routage pour informer les autres routeurs du réseau. L'envoi de ces mises à jour, appelées mises à jour déclenchées, est indépendant de l'envoi de mises à jour régulières par les routeurs RIP. Par exemple, les descriptions ci-dessous correspondent aux commandes utilisées pour configurer le routeur BHM illustré dans le schéma.

- `BHM(config)#`**`router rip`** – Sélectionne le protocole RIP comme protocole de routage
- `BHM(config-router)#`**`network 10.0.0.0`** – Spécifie un réseau directement connecté.
- `BHM(config-router)#`**`network 192.168.13.0`** – Spécifie un réseau directement connecté.

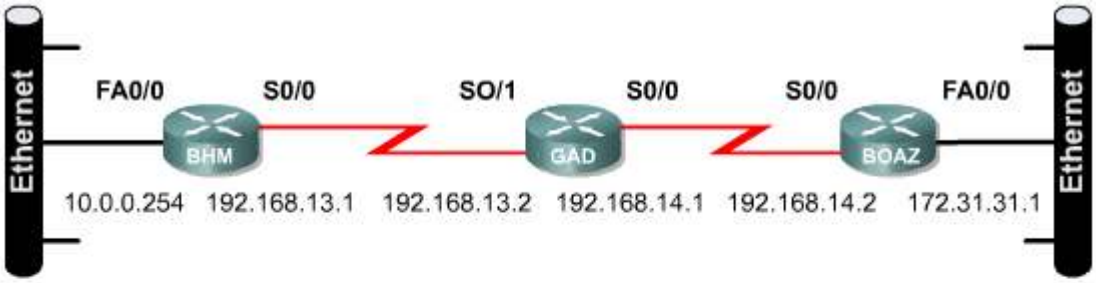
Les interfaces du routeur Cisco connectées aux réseaux 10.0.0.0 et 192.168.13.0 envoient et reçoivent les mises à jour RIP. Ces mises à jour de routage permettent au routeur d'apprendre la topologie du réseau par l'intermédiaire d'un routeur voisin exécutant également le protocole RIP.

Le protocole RIP doit être activé et les réseaux spécifiés. Les autres tâches sont facultatives. Voici la liste non exhaustive de ces tâches facultatives:

- Application de décalages aux métriques de routage
- Réglage des compteurs
- Spécification d'une version RIP
- Activation de l'authentification du protocole RIP
- Configuration du résumé de routes sur une interface
- Vérification du résumé de routes IP
- Désactivation du résumé de routes automatique
- Exécution simultanée d'IGRP et de RIP
- Désactivation de la validation des adresses IP sources
- Activation ou désactivation de la fonction «split horizon»
- Connexion du protocole RIP à un WAN

Pour activer le routage RIP, exécutez les commandes suivantes en commençant en mode de configuration globale:

- `Router(config)#`**`router rip`** – Active le processus de routage RIP
- `Router(config-router)#`**`network`***`numéro-réseau`* – Associe un réseau au processus de routage RIP




```
BHM(config)#router rip
BHM(config-router)#network 10.0.0.0
BHM(config-router)#network 192.168.13.0
```

```
GAD(config)#router rip
GAD(config-router)#network 192.168.14.0
GAD(config-router)#network 192.168.13.0
```

```
BOAZ(config)#router rip
BOAZ(config-router)#network 192.168.14.0
BOAZ(config-router)#network 172.31.0.0
```

b

Activité de TP

Exercice : Configuration du protocole RIP

Ce TP a pour objectif de configurer un système d'adressage IP en utilisant des réseaux de classe B et de configurer le protocole de routage dynamique RIP sur des routeurs

Activité de TP

Activité en ligne : RIP

Les étudiants vont examiner la topologie des routeurs avant de commencer le TP.

7.2 RIP

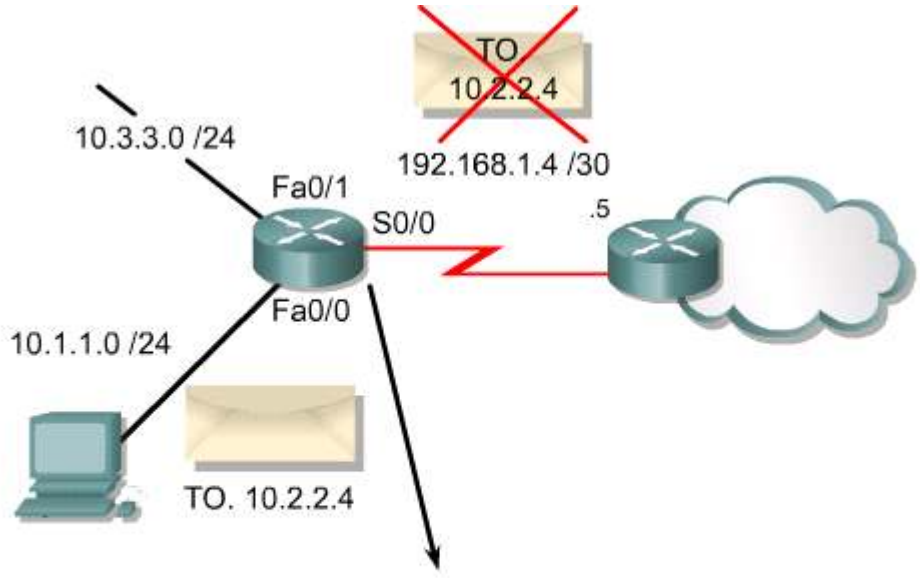
7.2.3 Utilisation de la commande ip classless

Un routeur peut parfois recevoir des paquets destinés à un sous-réseau inconnu ou à un réseau comportant des sous-réseaux directement connectés. Pour que la plate-forme logicielle Cisco IOS transmette ces paquets à la meilleure route SUPERNET possible, utilisez la commande **`ip classless`** en mode de configuration globale. Une route SUPERNET permet de couvrir un plus grand nombre de sous-réseaux avec une seule entrée. Par exemple, une entreprise utilise le sous-réseau 10.10.0.0 /16 complet, puis une route supernet pour 10.10.10.0 /24 serait 10.10.0.0 /16. La commande **`ip classless`** est activée par défaut à partir de la version 11.3 de la plate-forme logicielle CISCO IOS. Pour désactiver cette fonction, utilisez la forme **`no`** de cette commande.

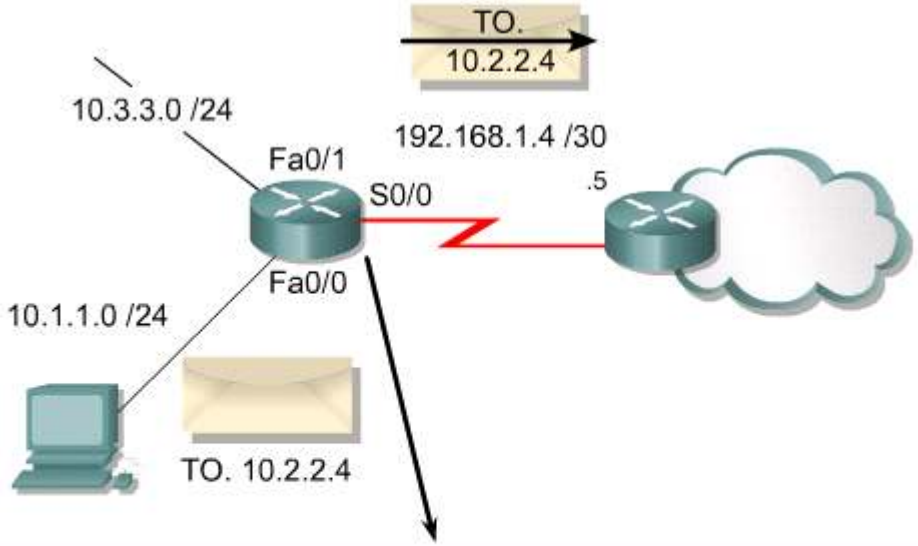
Lorsque cette fonction est désactivée, les paquets destinés à un sous-réseau inclus numériquement dans le système d'adressage de sous-réseau du routeur sont supprimés.

La commande «ip classless» n'affecte que le déroulement des processus de transmission de l'IOS. Elle n'affecte en rien le mode de création de la table de routage. Cette description constitue l'essence même du routage par classe. Si une partie du réseau principal est connue mais que le sous-réseau vers lequel le paquet s'achemine au sein du réseau principal est inconnu, le paquet est abandonné.

L'aspect le plus délicat de cette règle est que le routeur n'utilise la route par défaut que si la destination réseau principale n'existe pas dans la table de routage. Par défaut, un routeur suppose que tous les sous-réseaux d'un réseau directement connecté doivent se trouver dans la table de routage. Si un paquet reçu comporte une adresse de destination inconnue dans un sous-réseau inconnu d'un réseau directement attaché, le routeur suppose que le sous-réseau n'existe pas. Le routeur abandonnera donc le paquet même s'il existe une route par défaut. La configuration **`ip classless`** du routeur permet de résoudre ce problème. En effet, le routeur peut alors ignorer les frontières entre les classes de réseaux au sein de sa table de routage et acheminer tout simplement les données vers la route par défaut. [1] [2] [3]



Réseau de destination	Interface de sortie
10.1.1.0	Fa 0/0
10.3.3.0	Fa 0/1
0.0.0.0	S 0/0



Réseau de destination	Interface de sortie
10.1.1.0	Fa 0/0
10.3.3.0	Fa 0/1
0.0.0.0	S 0/0

```
GAD#configure terminal
GAD(config)#ip classless
```

Activité de TP

Activité en ligne : Utilisation du routage IP sans classe

Au cours de ce TP, l'étudiant va configurer le routeur pour qu'il puisse utiliser le routage IP sans classe lors de l'envoi de paquets.

7.2 RIP

7.2.4 Problèmes de configuration RIP fréquents

Les routeurs RIP doivent se fier aux routeurs voisins pour obtenir les informations réseau dont ils n'ont pas connaissance directement. Cette fonctionnalité est couramment appelée «routage par rumeur». Le protocole RIP utilise un algorithme de routage à vecteur de distance. Tous les protocoles de routage à vecteur de distance rencontrent des problèmes liés à la lenteur de la convergence. On parle de convergence lorsque tous les routeurs d'un interréseau utilisent les mêmes informations de routage.

On rencontre notamment des problèmes de boucles de routage et de métrique de mesure infinie. Ces problèmes entraînent des incohérences provoquées par les messages de mise à jour du routage avec des routes obsolètes propagées sur l'interréseau.

Pour réduire les boucles de routage et les problèmes de métrique de mesure infinie, le protocole RIP utilise les techniques suivantes:

- Métrique de mesure infinie
- Split horizon
- Poison reverse
- Compteurs de retenue
- Mises à jour déclenchées

Certaines de ces méthodes peuvent nécessiter une configuration alors que d'autres n'en ont jamais besoin ou très rarement.

Le nombre maximum de sauts pour le protocole RIP est 15. Les destinations situées au-delà de 15 sauts sont identifiées comme inaccessibles. Cette limite restreint considérablement l'utilisation de ce protocole dans les grands interréseaux mais permet d'éviter que le problème de « métrique de mesure infinie » ne provoque des boucles de routage sans fin.

La règle de «split horizon» est basée sur la théorie selon laquelle il n'est pas utile de renvoyer les informations relatives à une route en sens inverse. Dans certaines configurations réseau, il peut être nécessaire de désactiver la fonction split horizon.

La commande suivante permet de désactiver la fonction split horizon:

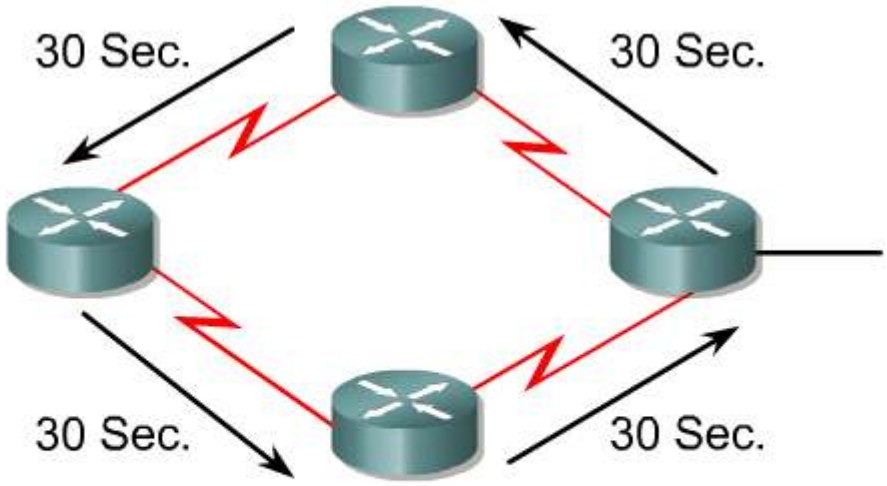
```
GAD(config-if)#no ip split-horizon
```

Le mécanisme des compteurs de retenue peut également nécessiter certaines modifications. Les compteurs de retenue permettent d'éviter la métrique de mesure infinie et d'améliorer le temps de convergence. La valeur par défaut du compteur de retenue RIP est de 180 secondes. Cette valeur permet d'éviter la mise à jour d'une route inférieure ainsi que l'installation d'une autre route valide. Il est possible de diminuer le compteur de retenue pour améliorer la convergence. Il faut cependant procéder avec la plus grande prudence. Dans l'idéal, il faudrait que la valeur du compteur corresponde au plus long temps de mise à jour possible pour l'interréseau. Dans l'exemple qu'illustre la figure 1, la boucle est constituée de quatre routeurs. Si le temps de mise à jour de chaque routeur est de 30 secondes, la boucle la plus longue serait de 120 secondes. Par conséquent, la valeur du compteur de retenue doit être légèrement supérieure à 120 secondes.

Utilisez la commande suivante pour changer l'intervalle de mise à jour:

```
Router(config-router)#timers basicupdate invalid holddown flush [sleeptime]
```

Un autre élément configurable affecte le temps de convergence : l'intervalle de mise à jour. Dans l'ISO CISCO, l'intervalle de mise à jour RIP par défaut est de 30 secondes. Il est possible de configurer ces intervalles, c'est-à-dire de les rallonger pour conserver la bande passante ou de les raccourcir pour réduire le temps de convergence.



30 + 30 + 30 + 30 = 120 secondes

Définir le compteur de retenue > 120 secondes

Dans le cadre des protocoles de routage, il faut également prendre en compte le cas où l'annonce des mises à jour de routage vers une interface spécifique n'est pas souhaitée. Lorsqu'une commande **network** est lancée pour un réseau donné, le protocole RIP commence immédiatement à envoyer des annonces à toutes les interfaces se trouvant dans la plage d'adresses réseau spécifiée. Pour contrôler l'échange de mises à jour de routage entre interfaces, l'administrateur réseau peut désactiver l'envoi des mises à jour de routage vers certaines interfaces en configurant la commande **passive-interface**. 2 3

```
RouterB#show ip route
Codes: C - connected, S - static, I - IGRP, R -
RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF
NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS
level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static
route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
R    192.168.1.0/24 [120/1] via 192.168.2.1,
00:00:02, Serial0/0
C    192.168.2.0/24 is directly connected,
Serial0/0
C    192.168.3.0/24 is directly connected,
FastEthernet0/0
RouterA#configure terminal
Enter configuration commands, one per line.  End
with Ctrl z.
RouterA(config)#router rip
RouterA(config-router)#passive-interface s0/0
RouterA(config-router)#^Z
RouterB#clear ip route *
RouterB#show ip route
Codes: C - connected, S - static, I - IGRP, R -
RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
```

```
IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF
NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS
level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static
route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
C    192.168.2.0/24 is directly connected,
Serial0/0
C    192.168.3.0/24 is directly connected,
FastEthernet0/0
```

Commande	Usage
GAD(config-router)# **passive-interface Fa0/0**	Configure une interface de manière à l'empêcher d'envoyer des paquets RIP.

RIP étant un protocole de diffusion (broadcast), l'administrateur réseau peut être amené à le configurer pour l'échange d'informations de routage sur un réseau ne prenant pas en charge la diffusion tel que Frame Relay. Dans ce type de réseau, le protocole RIP doit être informé sur les autres RIP voisins. Pour cela, utilisez la commande affichée dans la figure 4.

Commande	Usage
GAD(config-router)# **neighbor** *ip address*	Définit un routeur voisin avec lequel échanger des informations de routage.

Par défaut, la plate-forme logicielle Cisco IOS reçoit des paquets RIP Version 1 et 2 mais n'envoie que des paquets Version 1. L'administrateur réseau peut configurer le routeur pour qu'il ne reçoive et n'envoie que des paquets Version 1 ou pour qu'il n'envoie que des paquets Version 2. Pour configurer le routeur pour envoyer et recevoir des paquets d'une seule version, utilisez la commande de la figure 5.

Commande	Usage
GAD(config-router)#**version {1|2}**	Configure le logiciel afin qu'il puisse recevoir et envoyer les paquets RIP Version 1 ou Version 2.
GAD(config-if)#**ip rip send version 1**	Configure une interface afin qu'elle n'envoie uniquement que des paquets RIP Version 2.
GAD(config-if)#**ip rip send version 2**	Configure une interface afin qu'elle n'envoie uniquement que des paquets RIP Version 2.
GAD(config-if)#**ip rip send version 1 2**	Configure une interface pour envoyer seulement des paquets RIP version 1 ou 2.

Pour contrôler la façon dont les paquets reçus d'une interface sont traités, utilisez les commandes présentées dans la figure 6

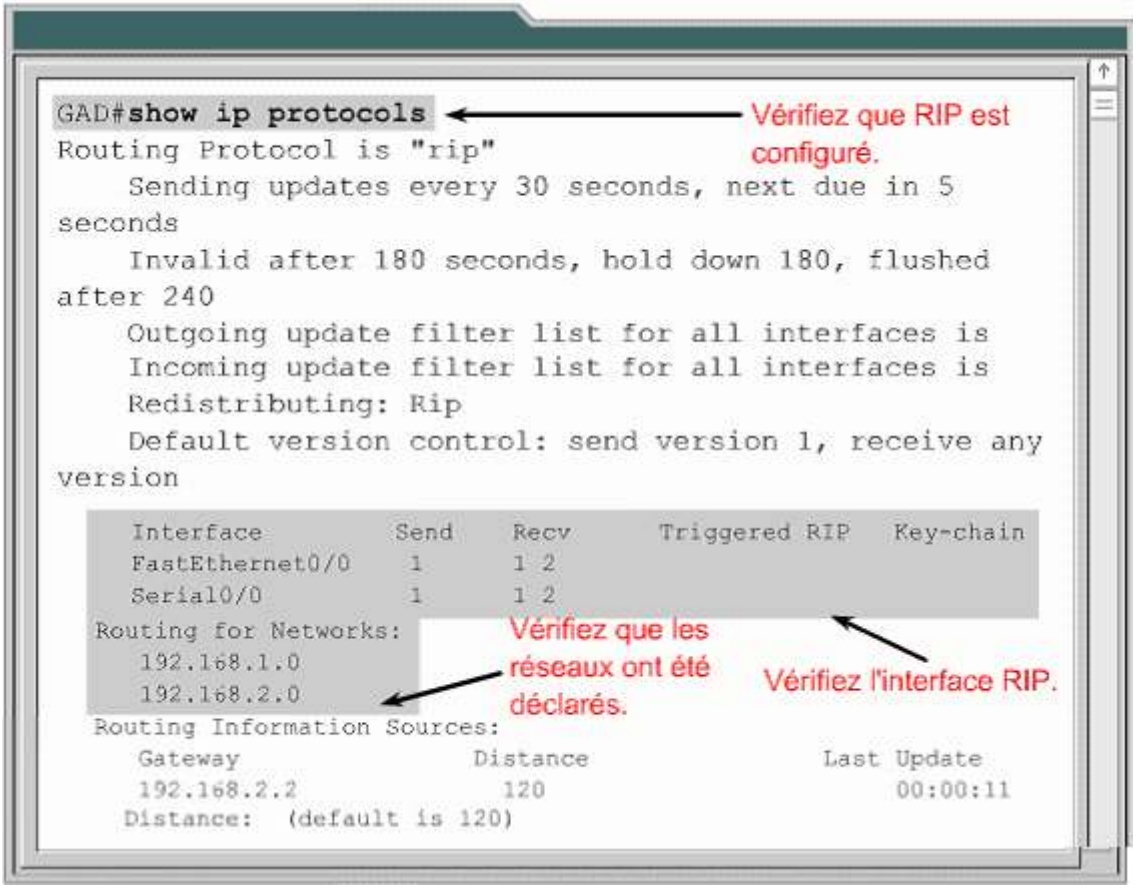
Commande	Usage
GAD(config-if)**#ip rip receive version 1**	Configure une interface afin qu'elle ne reçoive uniquement que des paquets RIP Version 1.
GAD(config-if)**#ip rip receive version 2**	Configure une interface afin qu'elle ne reçoive uniquement que des paquets RIP Version 2.
GAD(config-if)**#ip rip receive version 1 2**	Configure une interface afin qu'elle puisse recevoir des paquets RIP Version 1 ou Version 2.

7.2 RIP

7.2.5 Vérification de la configuration RIP

Vous pouvez utiliser plusieurs commandes pour vérifier que le protocole RIP est configuré correctement. Les deux plus répandues sont **`show ip route`** et **`show ip protocols`**.

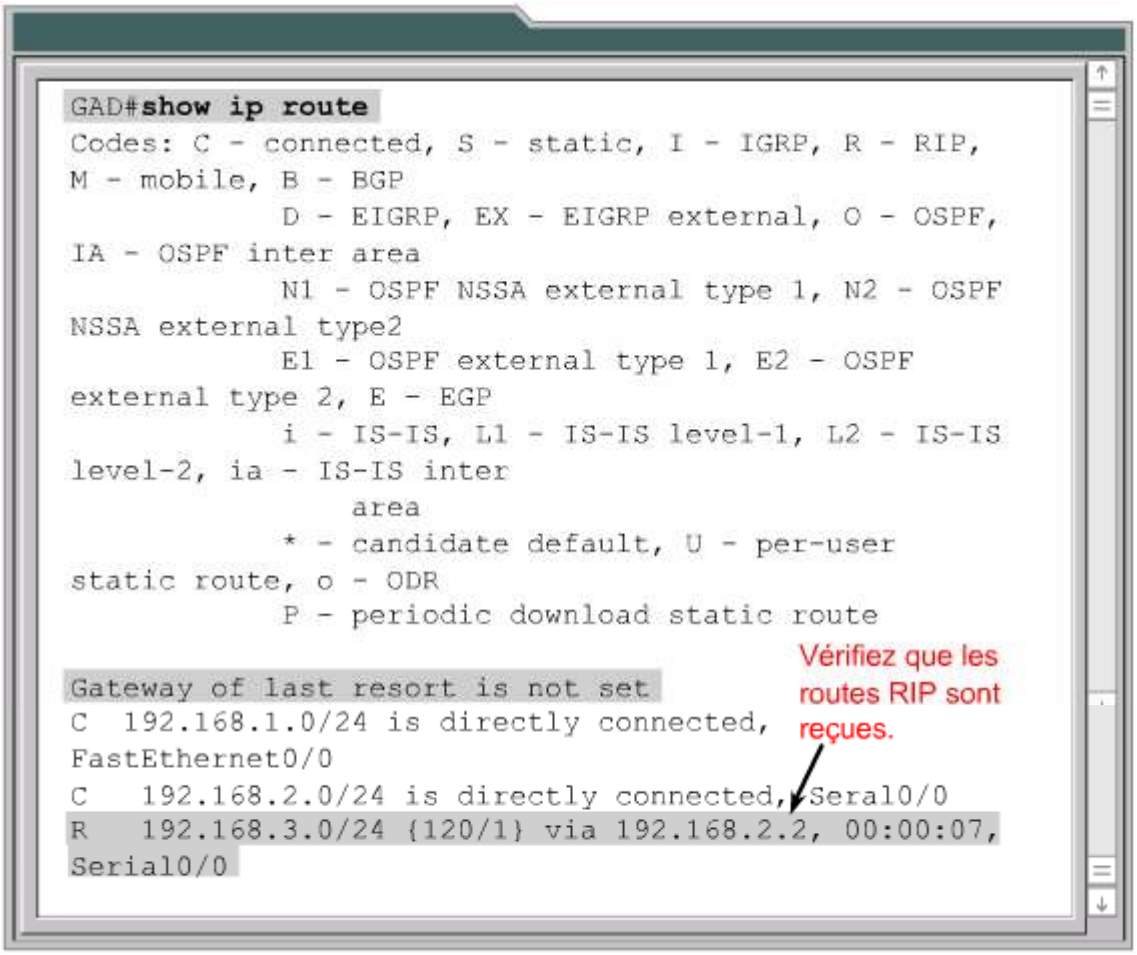
La commande **`show ip protocols`** affiche les protocoles de routage utilisés pour l'acheminement du trafic IP sur le routeur. 1



Ces informations peuvent être utilisées pour vérifier la plupart des configurations RIP, voire toutes. Les éléments de configuration les plus courants à vérifier sont les suivants:

- Est-ce que RIP est configuré?
- Est-ce que les interfaces appropriées envoient et reçoivent des mises à jour RIP?
- Est-ce que le routeur annonce les réseaux appropriés?

La commande **`show ip route`** peut être utilisée pour vérifier que les routes reçues par les voisins RIP figurent bien dans la table de routage. 2



Examinez les informations affichées par la commande et examinez les routes RIP signalées par “R”. N’oubliez pas qu’il va falloir un certain temps avant que le réseau converge, les routes n’apparaîtront donc pas immédiatement.

Des commandes supplémentaires permettent de vérifier la configuration RIP, par exemple:

- **show interface** *interface*
- **show ip interface***interface*
- **show running-config**

Activité de TP

Activité en ligne : Vérification de la configuration RIP

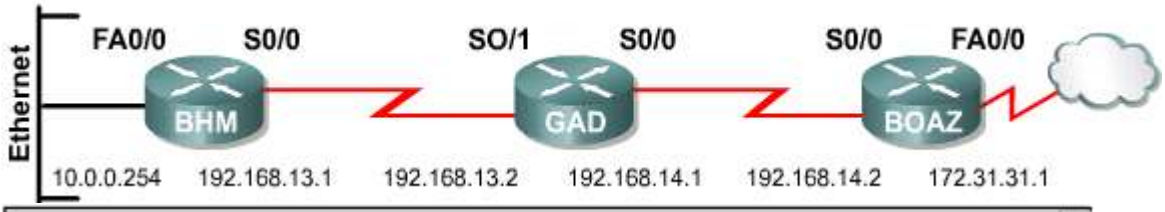
Au cours de ce TP, vous utiliserez des commandes show IOS pour vérifier le fonctionnement d'un routeur exécutant RIP.

7.2 RIP

7.2.6 Dépannage des problèmes de mise à jour RIP

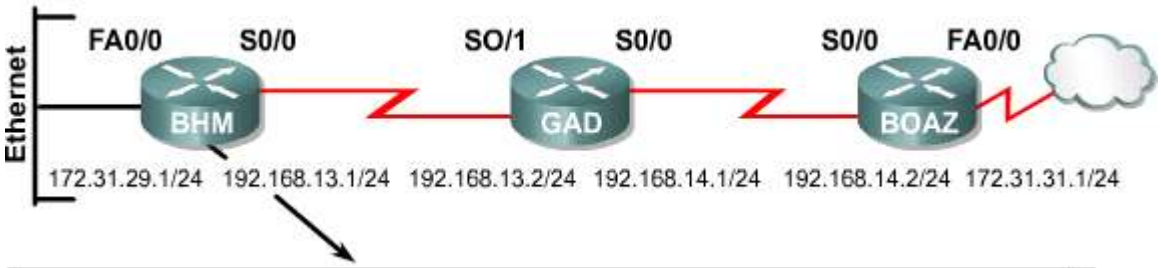
La plupart des erreurs de configuration RIP sont dues à une instruction réseau incorrecte, des réseaux non contigus ou des mises à jour split horizons. La commande **debug ip rip** est très efficace dans la résolution des problèmes de mise à jour RIP.

Elle permet d’afficher les mises à jour de routage RIP lors de leur envoi et de leur réception.



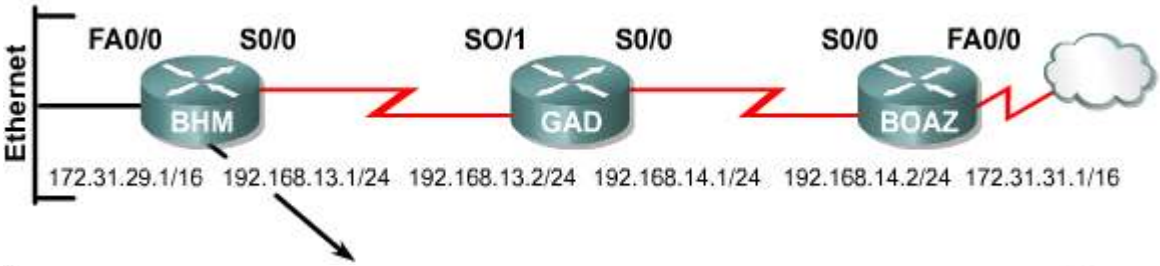

```
BHM#debug ip rip
RIP event debugging is on
BHM#
00:45:33: RIP: received v1 update from 192.168.13.2
on Serial0/0
00:45:33:        192.168.14.0 in 1 hop
00:45:33:        172.31.0.0 in 2 hop
00:45:33:        172.29.0.0 15 hops
00:45:36: RIP: sending v1 update to 255.255.255.255
via FastEthernet0/0 (10.0.0.254)
00:45:36:          network 192.168.13.0. metric 1
00:45:36:          network 192.168.14.0. metric 2
00:45:36:          network 172.31.0.0. metric 3
00:45:36:          network 172.29.0.0. metric 16
```

L'exemple de la figure 1 présente les informations provenant d'un routeur qui utilise la commande **debug ip rip** après avoir reçu une mise à jour RIP. Après avoir reçu et traité la mise à jour, le routeur envoie les informations récemment modifiées à ses deux interfaces RIP. Les informations affichées indiquent que le routeur utilise le protocole RIP version 1 et diffuse la mise à jour (adresse de broadcast 255.255.255.255). Le nombre entre parenthèses représente l'adresse source encapsulée dans l'en-tête IP de la mise à jour RIP.




```
BHM#debug ip rip
RIP event debugging is on
BHM#
7w2d: RIP:  received v1 update from 192.168.13.2 on
Serial 0/0
7w2d:         192.168.14.0 in 1 hop
7w2d:         172.31.0.0 in 2 hops
7w2d: RIP: sending v1 update to 255.255.255.255 via
Serial 0/0 (192.168.13.1)
7w2d:         network 172.31.0.0, metric 1
7w2d: RIP: sending v1 update to 255.255.255.255 via
F ast Ethernet0/0 (10.0.0.254)
7w2d:         network 192.168.13.0, metric 1
7w2d:         network 192.168.14.0, metric 2
```

Il faut rechercher plusieurs indicateurs clés dans les informations affichées par la commande **debug ip rip**. Cette commande permet de diagnostiquer des sous-réseaux contigus ou des réseaux en double. Par exemple, un des symptômes permettant d'identifier de tels problèmes serait un routeur annonçant une route avec une métrique inférieure à la métrique reçue pour ce réseau. 2 3




```
BHM#debug ip rip
RIP event debugging is on
BHM#
7w2d: RIP:  received v1 update from 192.168.13.2 on
Serial 0/0
7w2d:          192.168.14.0 in 1 hop
7w2d:          172.31.0.0 in 2 hops
7w2d: RIP: sending v1 update to 255.255.255.255 via
Serial 0/0 (192.168.13.1)
7w2d:          network 172.31.0.0, metric 1
7w2d: RIP: sending v1 update to 255.255.255.255 via
F ast Ethernet0/0 (10.0.0.254)
7w2d:          network 192.168.13.0, metric 1
7w2d:          network 192.168.14.0, metric 2
```

Les commandes ci-dessous permettent aussi de résoudre les problèmes RIP:

- **show ip rip database**
- **show ip protocols** {summary}
- **show ip route**
- **debug ip rip** {events}
- **show ip interface brief**

Activité de TP

Exercice : Dépannage RIP

Ce TP a pour but de configurer un système d'adressage IP avec des réseaux de classe B.

Activité de TP

Activité en ligne : Dépannage des problèmes de mise à jour RIP

Ce TP a pour but de réaliser la configuration de base du routeur Pretoria.

Activité de TP

Activité en ligne : Dépannage RIP

Dans cet exercice, les étudiants vont dépanner le protocole RIP sur les routeurs Gadsen et Birmingham.

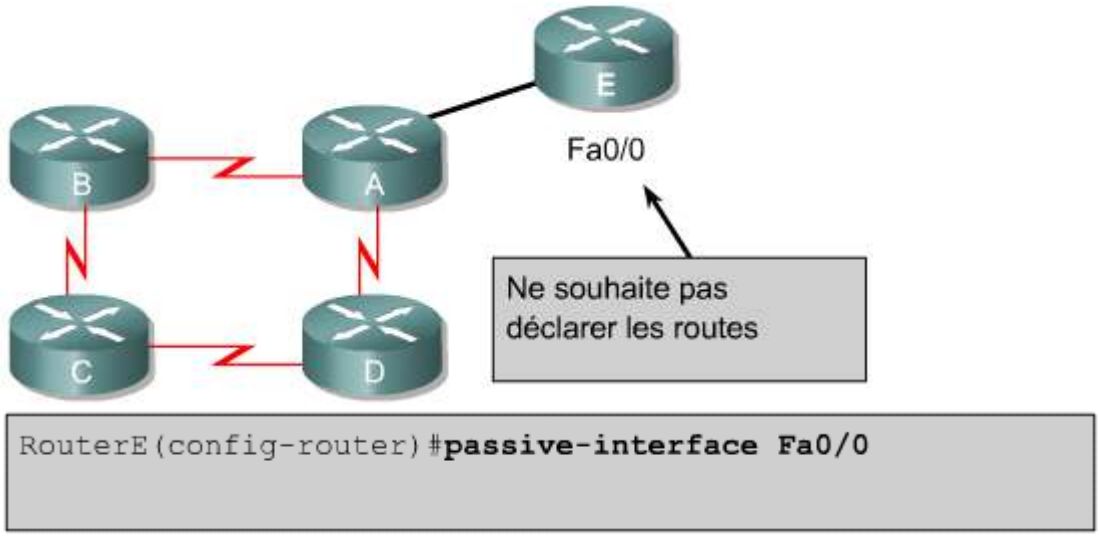
7.2 RIP

7.2.7 Comment empêcher les mises à jour du routage via une interface

Le filtrage de routes fonctionne par la régulation des routes entrées dans une table de routage ou annoncées. Ce fonctionnement n'a pas le même effet sur les protocoles de routage à état de liens que sur les protocoles à vecteur de distance. Un routeur exécutant un protocole à vecteur de distance annonce les routes en fonction du contenu de sa table de routage. Par conséquent, un filtre de route détermine quelles routes le routeur annonce à ses voisins.

D'autre part, les routeurs qui exécutent des protocoles de routage à état de liens déterminent les routes en fonction des informations de la base de données d'état de liens plutôt qu'avec les routes annoncées par le routeur voisin. Les filtres de route n'ont aucun effet sur les mises à jour de routage à état de liens ou sur la base de données à état de liens. Pour cette raison, les informations contenues dans ce document ne s'appliquent qu'aux protocoles de routage IP à vecteur de distance tels que RIP (Routing Information Protocol) et IGRP (Interior Gateway Routing Protocol).

La commande **`passive interface`** permet d'empêcher les routeurs d'envoyer des mises à jour de routage via une interface de routeur. Ceci permet d'empêcher les autres systèmes de ce réseau d'apprendre les routes de façon dynamique. Dans le diagramme 1, le routeur E utilise la commande **`passive interface`** pour empêcher l'envoie de mises à jour de routage.



Pour les protocoles RIP et IGRP, la commande **`passive interface`** empêche le routeur d'envoyer des mises à jour de routage à un voisin particulier tout en lui permettant d'écouter les mises à jour de routage provenant de ce même voisin. En empêchant l'envoi de messages de mises à jour de routage via une interface de routeur, les autres systèmes de ce réseau ne peuvent pas apprendre les routes de façon dynamique.

Activité de TP

Exercice : Comment empêcher les mises à jour du routage via une interface

L'objectif de ce TP est d'empêcher les mises à jour du routage via une interface pour réguler les routes annoncées.

Activité de TP

Activité en ligne : Comment empêcher les mises à jour du routage via une interface

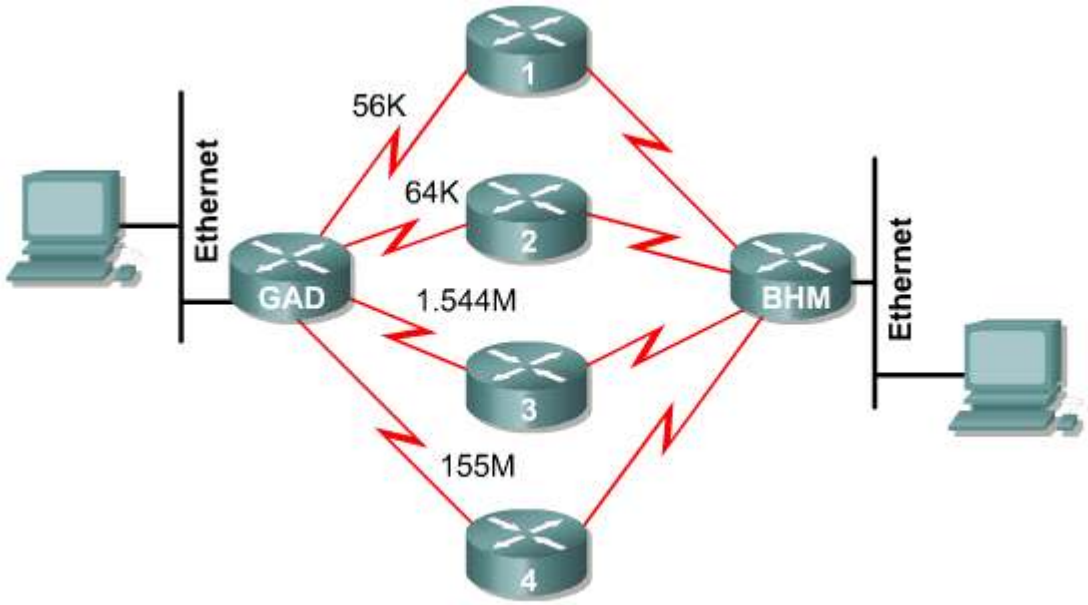
Au cours de ce TP, les étudiants vont apprendre à empêcher les mises à jour du routage via une interface pour réguler les routes annoncées et à observer les résultats.

7.2 RIP

7.2.8 Équilibrage de charge RIP

L'équilibrage de charge est un concept permettant à un routeur de bénéficier de plusieurs « meilleurs chemins » vers une destination donnée. Ces chemins peuvent être définis de manière statistique par un administrateur réseau ou calculés par un protocole de routage dynamique tel que RIP.

RIP est capable de gérer un équilibrage de charge sur plus de six chemins de coût égal avec quatre chemins par défaut. RIP réalise ce qu'on appelle un équilibrage de charge de recherche séquentielle. En d'autres termes, RIP envoie tour à tour les paquets sur les chemins parallèles.



La figure 1 présente un exemple de routes RIP à quatre chemins de coût égal. Au démarrage, le routeur utilise un pointeur d'interface qui pointe sur l'interface connectée au routeur 1. Ensuite, le pointeur d'interface boucle sur les interfaces et les routes d'une façon déterministe selon le modèle 1-2-3-4-1-2-3-4-1, etc. Comme la métrique utilisée pour le protocole RIP est le nombre de sauts, aucune importance n'est accordée au débit des liaisons. Par conséquent, le chemin présentant un débit de 56 Kbits/s ne sera pas privilégié par rapport à celui de 155 Mbits/s.

Il est possible de trouver les routes de coût égal à l'aide de la commande **`show ip route`**. Par exemple, la figure 2 illustre les informations affichées par la commande **`show ip route`** sur un sous-réseau particulier avec plusieurs routes.

Notez qu'il y a deux blocs descripteurs de réseau. Chaque bloc correspond à une route. Il y a également un astérisque (*) en regard d'une des entrées de bloc. Il s'agit de la route active utilisée pour le nouveau trafic.

```
Router#show ip route 10.0.0.0
  Routing entry for 10.0.0.0/8
  Known via "rip", distance 120, metric 1
  Redistributing via rip
  Advertised by rip (self originated)
  Last update from 192.168.75.7 on Serial1,
00:00:00 ago
  Routing Descriptor Blocks:
  * 192.168.57.7, from 192.168.57.7, 00:00:18 ago,
via Serial0
      Route metric is 1, traffic share count is 1
    192.168.75.7, from 192.168.75.7, 00:00:00 ago,
via Serial1
      Route metric is 1, traffic share count is 1
```

7.2 RIP

7.2.9 Équilibrage de charge sur plusieurs chemins

L'équilibrage de charge décrit la possibilité pour un routeur de transmettre des paquets vers une adresse IP de destination en utilisant plusieurs chemins. L'équilibrage de charge est un concept permettant à un routeur de bénéficier de plusieurs « meilleurs chemins » vers une destination donnée. Les chemins peuvent être définis de manière statistique ou calculés par un protocole de routage dynamique tel que RIP, EIGRP, OSPF et IGRP.

Source route distance administrative	Distance par défaut
Interface connectée	0
Route statique	1
Route sommaire EIGRP	5
BGP externe	20
Route interne EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
Route externe EIGRP	170
BGP interne	200
Inconnu	255

Lorsqu'un routeur apprend plusieurs routes vers un réseau spécifique, c'est la route avec la distance administrative la plus courte qui est ajoutée à la table de routage. 1 Le routeur doit parfois sélectionner une route parmi plusieurs, apprises via le même processus de routage, avec la même distance administrative. Dans ce cas, le routeur choisit le chemin de moindre coût ou présentant la métrique la plus basse vers la destination. Chaque processus de routage calcule son coût différemment et il peut être nécessaire de configurer les coûts manuellement pour réaliser l'équilibrage de charge.

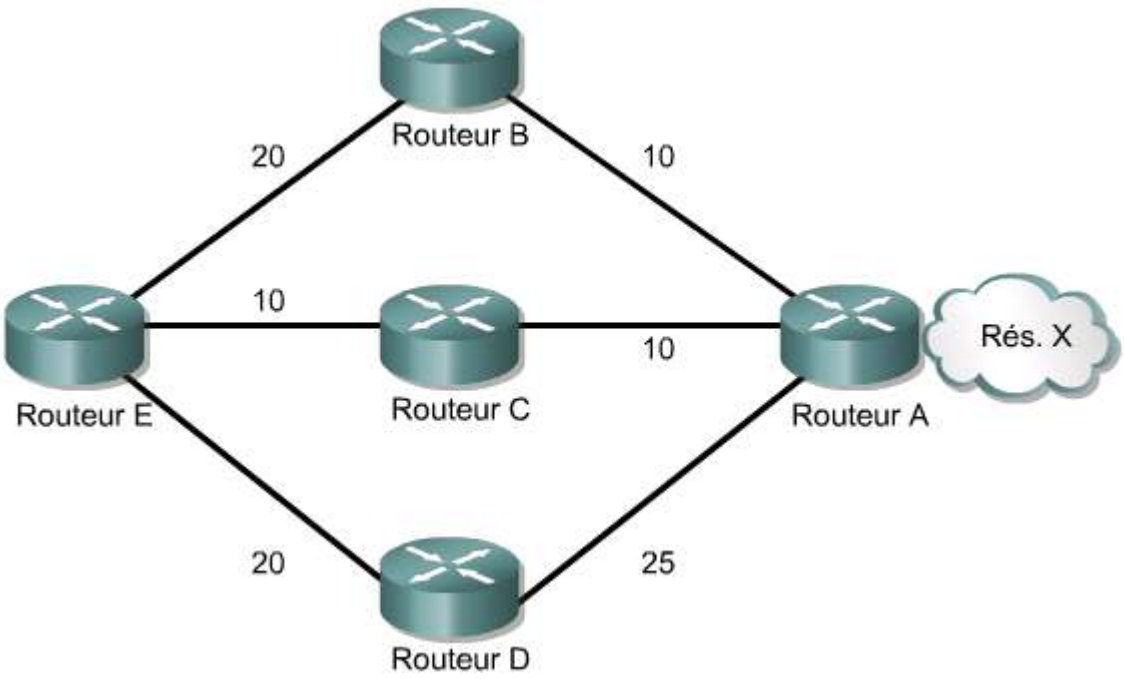
Si le routeur reçoit et installe plusieurs chemins avec la même distance administrative et le même coût vers une destination, l'équilibrage de charge peut se mettre en place. Il peut y avoir jusqu'à six routes de coût égal (limite imposée par Cisco IOS sur les tables de routage), mais certains protocoles IGP (Interior Gateway Protocols) ont leur propre limite. EIGRP autorise jusqu'à quatre routes de coût égal maximum.

Par défaut, la plupart des protocoles de routage IP installent au maximum quatre routes parallèles dans une table de routage. Les routes statiques installent toujours six routes. Toutefois, par défaut, BGP n'autorise qu'un seul chemin vers une destination.

Le nombre de chemins maximum peut varier selon une plage de un à six. Pour modifier le nombre maximum de chemins parallèles autorisés, utilisez la commande suivante en mode de configuration de routeur :

```
Router(config-router)#maximum-paths [nombre]
```

IGRP peut répartir la charge sur six liaisons inégales. Les réseaux RIP doivent avoir le même nombre de sauts pour répartir la charge alors que le protocole IGRP utilise la bande passante pour déterminer le mode d'équilibrage de charge.



Les trois modes d'accès au réseau X sont les suivants:

- E —> B —> A avec une métrique de 30
- E —> C —> A avec une métrique de 20
- E —> D —> A avec une métrique de 45

Le routeur E choisit le deuxième chemin ci-dessus, soit E-C-A avec une métrique de 20, puisqu'il s'agit du chemin de plus faible coût par rapport à 30 et à 45.

Cisco IOS offre deux méthodes d'équilibrage de charge pour le routage IP: équilibrage de charge par paquet et par destination. Si le processus de commutation est activé, le routeur peut changer de chemin à chaque nouveau paquet. Si la commutation «Fast Switching» est activée, une seule des routes sera mise en mémoire cache pour l'adresse de destination et les paquets de la trame acheminés vers un hôte spécifique prendront tous le même chemin. Les paquets en route vers un hôte différent sur le même réseau peuvent utiliser une autre route car l'équilibrage de charge du trafic est déterminé en fonction de la destination.

Par défaut les routeurs utilisent l'équilibrage de charge par destination, aussi appelé commutation «Fast Switching». Dans ce cas, la mémoire cache choisit la route des paquets sortants par un équilibrage de charge par destination plutôt que par paquet. Pour désactiver la commutation «Fast Switching», il faut utiliser la commande **`no ip route-cache`**. L'utilisation de cette commande a pour effet de gérer le trafic par un équilibrage de charge par paquet.

Activité de TP

Exercice : Équilibrage de charge sur plusieurs chemins

L'objectif de ce TP est de configurer l'équilibrage de charge sur plusieurs chemins.

Activité de TP

Activité en ligne : Équilibrage de charge sur plusieurs chemins

Au cours de ce TP, les étudiants vont répartir la charge sur plusieurs chemins et observer le processus d'équilibrage de charge.

Activité de média interactive

Glisser-Positionner : Distances administratives

À la fin de cette activité, l'étudiant sera en mesure de comprendre les distances administratives.

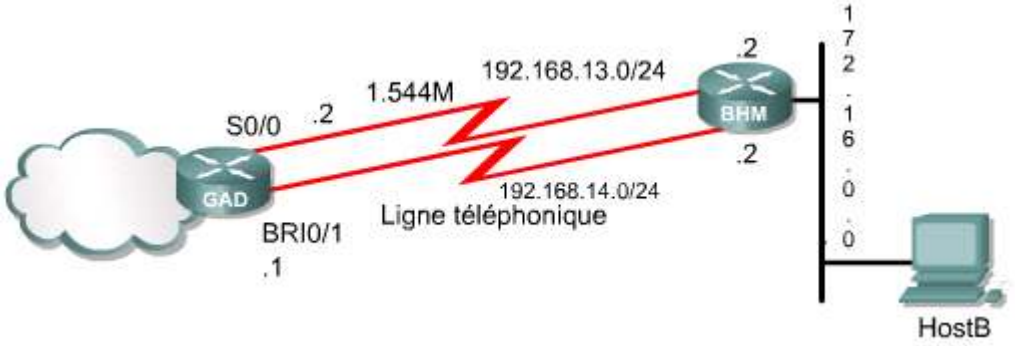
7.2 RIP

7.2.10 Intégration des routes statiques avec le protocole RIP

Les routes statiques sont des routes personnalisées (définies par l'utilisateur) qui obligent les paquets à emprunter un chemin défini pour se déplacer entre une source et une destination. Le rôle de ces routes est fondamental lorsque la plate-forme logicielle de l'ISO CISCO ne connaît pas de route vers une destination particulière. Elles permettent également de spécifier une « passerelle de dernier recours, plus communément appelée «route par défaut». Lorsqu'un paquet doit être envoyé vers un sous-réseau qui ne figure pas explicitement dans la table de routage, ce paquet est transmis via la route par défaut.

Un routeur RIP peut recevoir une route par défaut via une mise à jour envoyée par un autre routeur RIP. Le routeur peut aussi générer lui-même la route par défaut.

Pour supprimer les routes statiques, il suffit d'entrer la commande **`no ip route`** en mode de configuration globale. L'administrateur peut remplacer une route statique par des informations de routage dynamique en ajustant les valeurs de distance administrative. Chaque protocole de routage dynamique comporte une distance administrative par défaut. Il est possible d'indiquer qu'une route statique est moins recommandée qu'une route apprise de façon dynamique si la distance administrative pas défaut de la route statique est supérieure à celle de la route dynamique. Notez qu'après que la route statique vers le réseau 172.16.0.0 via 192.168.14.2 ait été entrée, la table de routage ne l'a pas montrée. Seule la route dynamique apprise par l'intermédiaire de RIP est présente. Cela est du à ce que la distance administrative est plus élevée (130) pour la route statique. A moins que la route RIP via S0/0 ne soit plus opérationnelle, la route statique ne sera pas installée dans la table de routage. 1

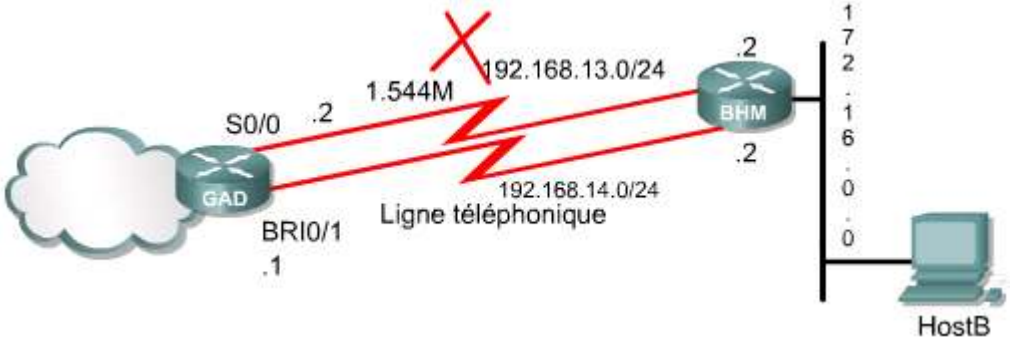



```
GAD#configure terminal
GAD(config)#ip route 172.16.0.0 255.255.0.0
192.168.14.2 130
GAD#show ip route
Codes: C - connected, s - static, I - IGRP, R - RIP,
M - mobile, B - BGP
            D - EIGRP, EX - EIGRP external, O -
OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 -
```

```
OSPF NSSA external type 2
            E 1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP
             i - IS-IS, L1 - IS-IS level - 1, L2 -
IS-IS level -2, ia - IS-IS inter area
             * - candidate default, U - per -user
static route, o - ODR
             p - periodic downloaded static route
    Gateway of last resort is not set
     C      192.168.13.0/24 is directly connected,
Serial 0/0
     C      192.169.14.0/24 is directly connected,
BRI0/1
     R      172.16.0.0/16 [120/1] via 192.16.13.2,
00:00:24, Serial0/0
```

Les routes statiques qui pointent vers une interface seront annoncées via le routeur RIP propriétaire de la route statique et ces routes seront propagées via l'interréseau. En effet, les routes statiques qui pointent vers une interface sont considérées dans la table de routage comme connectées et perdent de ce fait leur caractère statique lors de la mise à jour. Si une route statique est affectée à une interface non définie dans le processus RIP, via une commande **`network`**, RIP n'annonce pas cette route, à moins qu'une commande **`redistribute static`** ne soit spécifiée dans le processus RIP.

Lorsqu'une interface tombe en panne, toutes les routes statiques pointant vers cette interface sont supprimées de la table de routage IP. De même, lorsqu'un logiciel ne trouve plus de saut suivant valide pour l'adresse spécifiée dans la route statique, cette dernière est supprimée de la table de routage IP.




```
GAD#show ip route
Codes: C - connected, s - static, I - IGRP, R - RIP,
M - mobile, B - BGP
             D - EIGRP, EX - EIGRP external, O -
OSPF, IA - OSPF inter area
            N1 - OSPF NSSA external type 1, N2 -
OSPF NSSA external type 2
            E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP
```

```
            i - IS-IS, L1 - IS-IS level - 1, L2 -
IS-IS level -2, ia - IS-IS inter area
            * - candidate default, U - per -user
static route, o - ODR
            p - periodic downloaded static route

Gateway of last resort is not set

     C      192.168.113.0/24 is directly connected,
     C      192.168.113.0/24 is directly connected,
Serial 0/0
     C      192.169.14.0/24 is directly connected,
BRI0/1
     R      172.16.0.0/16 [120/1] via 192.16.14.2
```

Dans la figure 2, une route statique a été configurée sur le routeur GAD pour remplacer la route RIP en cas de défaillance du processus de routage RIP. Ce type de route s'appelle une route statique flottante. La route statique flottante a été configurée en définissant une distance administrative par défaut sur la route statique (130) supérieure à la distance administrative RIP par défaut (120). Le routeur BHM doit aussi être configuré avec une route par défaut.

Commande	Usage
ip route destination mask {interface/nexthop}	Établit une route statique.

Pour configurer une route statique, utilisez la commande de la figure 3 en mode de configuration globale.

Activité de TP

Activité en ligne : Intégration des routes statiques avec le protocole RIP

Au cours de ce TP, les étudiants vont activer le protocole RIP pour la propagation des routes statiques.

7.3 IGRP

7.3.1 Caractéristiques du protocole IGRP

Le protocole IGRP est un protocole IGP (Interior Gateway Protocol) à vecteur de distance. Les protocoles de routage à vecteur de distance comparent les routes de façon mathématique en mesurant les distances. Cette mesure est appelée vecteur de distance. Les routeurs utilisant des protocoles à vecteur de distance doivent envoyer, à intervalles réguliers, une partie ou l'intégralité de leur table de routage sous forme de message de mise à jour à tous les routeurs voisins. Lors de la diffusion des informations de routage sur l'ensemble du réseau, les routeurs exécutent les fonctions suivantes:

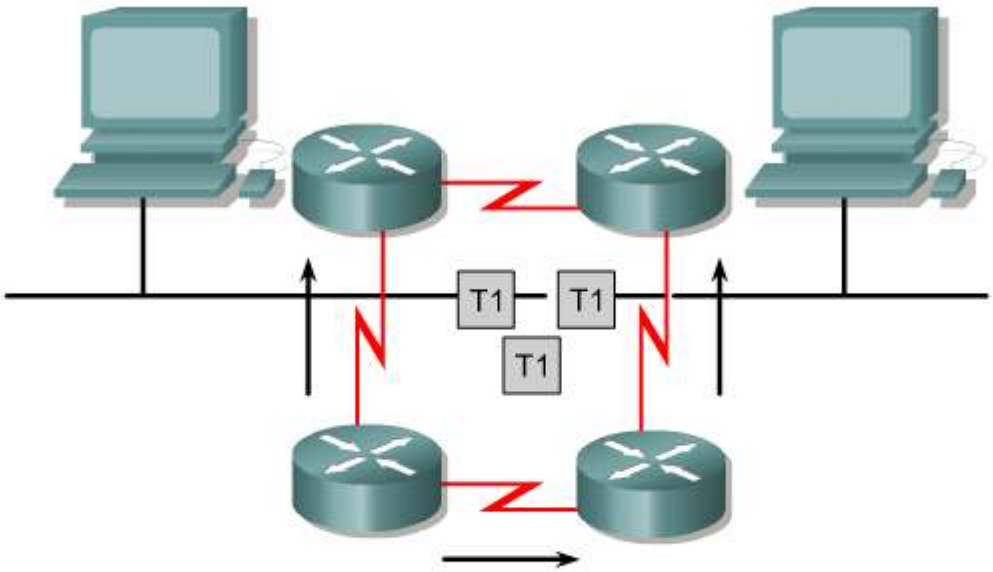
- Identification de nouvelles destinations
- Apprentissage des pannes

Le protocole IGRP est un protocole de routage à vecteur de distance mis au point par Cisco. Il envoie les mises à jour de routage toutes les 90 secondes et donne aux réseaux des informations sur un système autonome particulier. Les principales caractéristiques de la conception du protocole IGRP sont les suivantes:

- Polyvalence lui permettant de traiter automatiquement des topologies complexes et indéfinies
- Flexibilité nécessaire à la segmentation avec des caractéristiques différentes en termes de bande passante et de délai
- Évolutivité lui permettant de fonctionner sur des réseaux de très grande taille

Le protocole de routage IGRP utilise par défaut la bande passante et le délai comme métriques. Par ailleurs, le protocole IGRP peut être configuré de manière à utiliser une combinaison de variables pour la détermination d'une métrique composée. Ces variables sont les suivantes:

- Bande passante
- Délai
- Charge
- Fiabilité



- Une métrique composée sélectionne le chemin.
- La vitesse est le facteur principal.

Activité de média interactive

Case à cocher : RIP et IGRP

À la fin de cette activité, l'étudiant sera en mesure de comprendre les protocoles RIP et IGRP

7.3 IGRP

7.3.2 Métriques du protocole IGRP

La commande **`show ip protocols`** affiche les paramètres, les filtres et les informations réseau concernant les protocoles de routage utilisés sur le routeur. Les coefficients K1 à K5 apparaissent sur le graphique. Ils sont utilisés par l'algorithme pour calculer la métrique de routage IGRP. Par défaut, les valeurs des coefficients K1 et K3 sont établies à 1 et les coefficients K2, K4 et K5 sont fixés à 0.

Cette métrique composée est plus précise que la mesure du nombre de sauts utilisée par le protocole RIP lors de la sélection d'un chemin vers la destination. Le chemin présentant la valeur métrique la plus petite constitue la meilleure route.

Les métriques utilisées par le protocole IGRP sont les suivantes:

- **Bande passante** – Valeur de bande passante la plus faible sur le chemin
- **Délai** – Délai d'interface global le long du chemin
- **Fiabilité** – Fiabilité de la liaison vers la destination, déterminée par l'échange de messages de veille
- **Charge** – Charge d'une liaison vers la destination, en bits par seconde

Le protocole IGRP utilise une métrique composée. Celle-ci est basée sur la bande passante, le délai, la charge et la fiabilité. Seuls la bande passante et le délai sont pris en compte par défaut. Les autres paramètres ne sont pris en considération que s'ils sont activés via la configuration. Le délai et la bande passante ne sont pas des valeurs mesurées mais des valeurs définies au moyen des commandes d'interface de délai et de bande passante. Dans l'exemple, la commande **`show ip route`** affiche les valeurs métriques IGRP entre crochets. Une liaison avec une bande passante plus élevée aura une métrique inférieure, tout comme une route présentant un délai global plus bas. 1

```
Router>show ip protocols
Routing Protocol is igrp 300
  Sending updates every 90 seconds, next due in 55
seconds
  Invalid after 270 seconds, hold down 280, flushed
after 360
  Outgoing update filter list for all interfaces is
not set
  Incoming update filter list for all interfaces is
not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  IGRP maximum hopcount 100
  IGRP maximum metric variance 1
  Redistributing igrp 300
  Routing for Networks:
    183.8.0.0
    144.253.0.0
  Routing Information Sources
    Gateway                 Distance        Last
Update
    144.253.100.1           100              0:00:52
    183.8.128.12            100              0:00:43
    183.8.64.130            100              0:01:02
  Distance: (default is 100)
-- More --
```

```
Router A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP
     D - EIGRP,EX - EIGRP external, O - OSPF, IA - OSPF
inter area
N1 - OSPF NSSA external type 1, N2 - OSPF  NSSA external
type 2
E1 - OSPF external type 1, E2 - OSPF exteranl type 2, E -
EGP
i - IS-IS, L1 - IS_IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
p - periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.2.0/24 is directly connected, Serial0/0
I 192.168.3.0/24 [100/80135] via 192.168.2.2, 00:00:30,
Serial0/0
```

7.3 IGRP

7.3.3 Routes IGRP

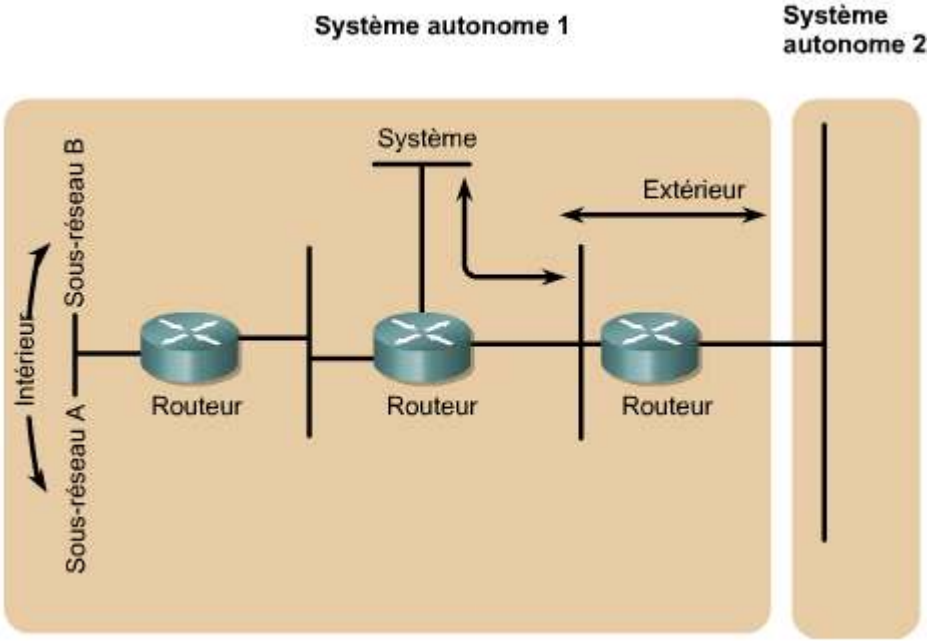
Le protocole IGRP annonce trois types de routes:

- Intérieure
- Système
- Extérieure

Intérieure
Les routes intérieures sont des routes situées entre les sous-réseaux d'un réseau relié à une interface de routeur. Si le réseau relié à un routeur n'est pas divisé en sous-réseaux, le protocole IGRP n'annonce pas les routes intérieures.

Système
Les routes système sont les routes menant à d'autres réseaux au sein d'un système autonome. La plate-forme logicielle IOS Cisco calcule les routes système en fonction des interfaces réseau directement connectées et des informations sur les routes système fournies par d'autres routeurs ou serveurs d'accès utilisant le protocole IGRP. Les routes système ne contiennent pas d'information sur les sous-réseaux.

Extérieure
Les routes extérieures sont des routes menant à des réseaux extérieurs au système autonome, et qui sont utilisées lorsqu'une passerelle de dernier recours est envisagée. La plate-forme logicielle IOS Cisco sélectionne une passerelle de dernier recours dans la liste des routes extérieures fournie par le protocole IGRP. Elle utilise la passerelle (routeur) de dernier recours s'il n'existe pas de meilleure route et si la destination n'est pas un réseau connecté. Si le système autonome est muni de plusieurs connexions à un réseau externe, les différents routeurs peuvent choisir des routes extérieures différentes comme passerelle de dernier recours.



Activité de média interactive

Case à cocher : Routes IGRP

À la fin de cette activité, l'étudiant sera en mesure de comprendre les routes IGRP.

7.3 IGRP

7.3.4 Caractéristiques de stabilité du protocole IGRP

Le protocole IGRP offre plusieurs fonctions conçues pour améliorer sa stabilité, notamment:

- Gels
- Split horizon
- Mises à jour en mode poison reverse

Gels
Les gels servent à empêcher les messages de mise à jour périodiques de rétablir une route susceptible de ne pas être active. Lorsqu'un routeur tombe en panne, les routeurs voisins le détectent grâce à l'absence de messages de mise à jour périodiques.

Split horizon
n'est pas utile de renvoyer les informations relatives à une route en sens inverse. Elle vise à empêcher les boucles de routage entre routeurs adjacents

Mises à jour en mode «poison reverse»
Les mises à jour en mode « poison reverse » sont utilisées pour empêcher les boucles de routages à plus grande échelle. En règle générale, les augmentations au niveau des métriques de routage signalent des boucles de routage. Des mises à jour en mode « poison reverse » sont alors envoyées pour fermer la route et la mettre en état de gel. Dans le cadre du protocole IGRP, les mises à jour de ce type ne sont envoyées que si le facteur d'augmentation d'une métrique de route est de 1.1 ou plus.

Le protocole IGRP gère également un certain nombre de compteurs et de variables contenant des intervalles de temps. Il existe notamment un compteur de mise à jour, un compteur de temporisation, un compteur de retenue et un compteur d'annulation.

Le compteur de mise à jour indique la fréquence d'envoi des messages de mise à jour du routage. La valeur par défaut IGRP de cette variable est de 90 secondes.

Le compteur de temporisation indique le laps de temps au bout duquel un routeur doit déclarer une route non valide en l'absence de messages de mise à jour la concernant. La valeur par défaut IGRP de cette variable correspond à trois fois la valeur du compteur de mise à jour.

Le compteur de retenue indique le laps de temps pendant lequel les informations relatives aux routes non optimales sont ignorées. La valeur par défaut IGRP de cette variable correspond à trois fois la valeur du compteur de mise à jour plus dix secondes.

Enfin, le compteur d'annulation indique le laps de temps devant s'écouler avant la suppression d'une route dans la table de routage. La valeur par défaut IGRP de cette variable correspond à sept fois la valeur du compteur de mise à jour du routage.

Le protocole IGRP montre actuellement ses faiblesses ; en effet, il ne prend pas en charge les masques de sous-réseau de longueur variable (VLSM). Plutôt que de développer une deuxième version de ce protocole, Cisco exploite le succès obtenu par ce dernier en introduisant le protocole Enhanced IGRP.

```
RouterB#show ip protocols
Routing Protocol is "igrp 101"
 Sending updates every 90 seconds, next due in 51
seconds
 Invalid after 270 seconds, hold down 280, flushed
after 630
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 IGRP maximum hopcount 100
 IGRP maximum metric variance 1
 Redistributing: igrp 101
 Routing for Networks:
  192.168.2.0
  192.168.3.0
 Routing Information Sources:
  Gateway    Distance    Last Update
  192.168.2.1     100    00:00:54
 Distance: (default is 100)
```

7.3 IGRP

7.3.5 Configuration du protocole IGRP

Pour configurer le processus de routage IGRP, utilisez la commande de configuration **`router igrp`**. Pour arrêter un processus de routage IGRP, utilisez la forme **`no`** de cette commande. 1

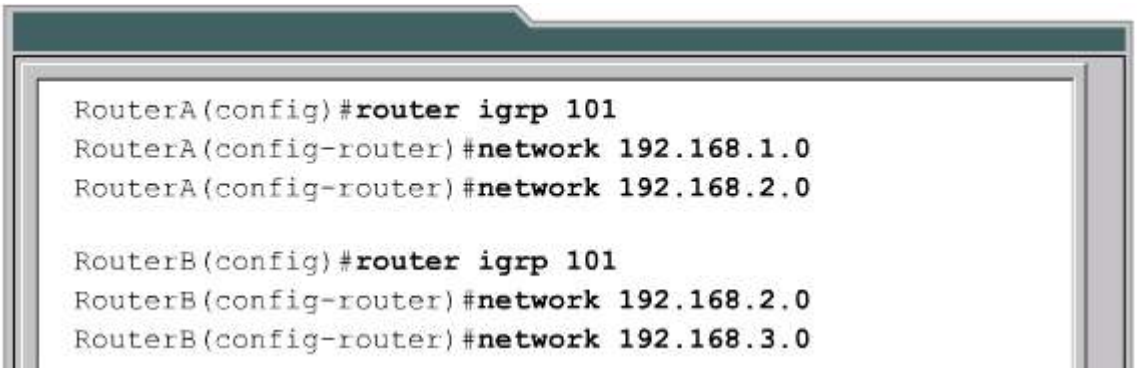
```
RouterA(config)#router igrp 101
RouterA(config-router)#network 192.168.1.0
RouterA(config)#no router igrp 101
```

```
RouterA(config)#router igrpnuméro_système_autonome
RouterA(config)#no router igrpnuméro_système_autonome
```

Le numéro de système autonome identifie le processus IGRP. Il sert également à marquer les informations de routage.

Pour indiquer une liste de réseaux pour les processus de routage IGRP, utilisez la commande de configuration de routeur **network**. Pour supprimer une entrée, utilisez la forme **no** de cette commande.

La figure 2 est un exemple de configuration du protocole IGRP avec le système autonome 101.



Activité de TP

Exercice : Configuration du protocole IGRP

Ce TP a pour but de configurer un système d'adressage IP avec des réseaux de classe B.

Activité de TP

Activité en ligne : Configuration du protocole IGRP

Au cours de ce TP, les étudiants apprendront à configurer le protocole IGRP.

7.3 IGRP

7.3.6 Migration de RIP vers IGRP

Avec l'introduction du protocole IGRP au début des années 80, Cisco Systems a été la première société à résoudre les problèmes liés à l'utilisation de RIP pour acheminer des datagrammes entre des routeurs internes. Le protocole IGRP détermine le meilleur chemin via l'interréseau en examinant la bande passante et le délai des réseaux entre les routeurs. Il converge plus rapidement que RIP, ce qui permet d'éviter les boucles de routage générées par un désaccord concernant le prochain saut de routage à effectuer. Par ailleurs, IGRP n'est pas soumis à la même limite du nombre de sauts que RIP. Grâce à cela et à d'autres améliorations par rapport à RIP, le protocole IGRP a permis de déployer un grand nombre d'interréseaux complexes, de grande taille et aux topologies variées.

Pour passer de RIP à IGRP, suivez la procédure ci-dessous:

```
RouterA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M
- mobile, B - BGP
   D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
   E1 - OSPF external type 1, E2 - OSPF external type
2, E - EGP
   i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area
   * - candidate default, U - per-user static route, o
- ODR
   P - periodic downloaded static route

Gateway of last resort is not set

C   192.168.1.0/24 is directly connected, Loopback0
C   192.168.2.0/24 is directly connected, Serial0/0
R   192.168.3.0/24 [120/1] via 192.168.2.2, 00:01:09,
Serial0/0
```

```
RouterB#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M
- mobile, B - BGP
   D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
   E1 - OSPF external type 1, E2 - OSPF external type
2, E - EGP
   i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area
   * - candidate default, U - per-user static route, o
- ODR
   P - periodic downloaded static route

Gateway of last resort is not set


R   192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:28,
Serial0/0
C   192.168.2.0/24 is directly connected, Serial0/0
C   192.168.3.0/24 is directly connected,
FastEthernet0/0
```

1. VEntrez la commande **`show ip route`** pour vérifier le protocole RIP sur les routeurs à convertir. 1 2

2. Configurez le protocole IGRP sur les routeurs A et B. 3

```
Entered on Router A

RouterA#configure terminal
RouterA(config)#router igrp 101
RouterA(config-router)#network 192.168.1.0
RouterA(config-router)#network 192.168.2.0


Entered on Router B

RouterB#configure terminal
RouterB(config)#router igrp 101
RouterB(config-router)#network 192.168.2.0
RouterB(config-router)#network 192.168.3.0
```

3. Entrez la commande **`show ip protocols`** sur les routeurs A et B. 4 5

```
RouterA#show ip protocols
Routing Protocol is "rip"
 Sending updates every 30 seconds, next due in 2
seconds
 Invalid after 180 seconds, hold down 180, flushed
after 240
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Redistributing: rip
 Default version control: send version 2, receive
version 2
   Interface    Send Recv Triggered RIP Key-chain
   FastEthernet0/0 2  2
   Serial0/0    2  2
 Routing for Networks:
   192.168.1.0
   192.168.2.0
```

```
 Routing Information Sources:
  Gateway    Distance    Last Update
  192.168.2.2      120    00:00:21
 Distance: (default is 120)

Routing Protocol is "igrp 101"
 Sending updates every 90 seconds, next due in 45
seconds
 Invalid after 270 seconds, hold down 280, flushed
after 630
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 IGRP maximum hopcount 100
 IGRP maximum metric variance 1
 Redistributing: igrp 101
 Routing for Networks:
  192.168.1.0
  192.168.2.0
 Routing Information Sources:
  Gateway    Distance    Last Update
  192.168.2.2      100    00:00:38
 Distance: (default is 100)
```

4. Entrez la commande **`show ip route`** sur les routeurs A et B.

```
RouterB#show ip protocols
Routing Protocol is "rip"
 Sending updates every 30 seconds, next due in 24
seconds
 Invalid after 180 seconds, hold down 180, flushed
after 240
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Redistributing: rip
 Default version control: send version 2, receive
version 2
   Interface    Send Recv Triggered RIP Key-chain
   FastEthernet0/0 2  2
   Serial0/0    2  2
 Routing for Networks:
  192.168.2.0
  192.168.3.0
```

```
 Routing Information Sources:
  Gateway    Distance    Last Update
  192.168.2.1      120    00:00:06
 Distance: (default is 120)

Routing Protocol is "igrp 101"
 Sending updates every 90 seconds, next due in 60
seconds
 Invalid after 270 seconds, hold down 280, flushed
after 630
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 IGRP maximum hopcount 100
 IGRP maximum metric variance 1
Redistributing: igrp 101
 Routing for Networks:
  192.168.2.0
  192.168.3.0
 Routing Information Sources:
  Gateway    Distance    Last Update
  192.168.2.1      100    00:01:17
 Distance: (default is 100)
```

```
RouterA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M
- mobile, B - BGP
   D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
   E1 - OSPF external type 1, E2 - OSPF external type
2, E - EGP
   i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area
   * - candidate default, U - per-user static route, o
- ODR
   P - periodic downloaded static route

Gateway of last resort is not set

C   192.168.1.0/24 is directly connected,
FastEthernet0/0
C   192.168.2.0/24 is directly connected, Serial0/0
I   192.168.3.0/24 [100/80135] via 192.168.2.2,
00:00:36, Serial0/0
```

```
RouterB#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M
- mobile, B - BGP
   D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
   E1 - OSPF external type 1, E2 - OSPF external type
2, E - EGP
   i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area
   * - candidate default, U - per-user static route, o
- ODR
   P - periodic downloaded static route

Gateway of last resort is not set

I  192.168.1.0/24 [100/8486] via 192.168.2.1,
00:01:05, Serial0/0
C  192.168.2.0/24 is directly connected, Serial0/0
C  192.168.3.0/24 is directly connected,
FastEthernet0/0
```

Activité de TP

Exercice : Routage par défaut avec les protocoles RIP et IGRP

L'objectif de ce TP est de configurer une route par défaut et d'utiliser le protocole RIP pour transmettre cette information aux autres routeurs.

Activité de TP

Activité en ligne : Configuration du routage par défaut avec les protocoles RIP et IGRP

Au cours de ce TP, les étudiants configureront une route par défaut et utiliseront le protocole RIP pour transmettre cette information aux autres routeurs.

7.3 IGRP

7.3.7 Vérification de la configuration IGRP

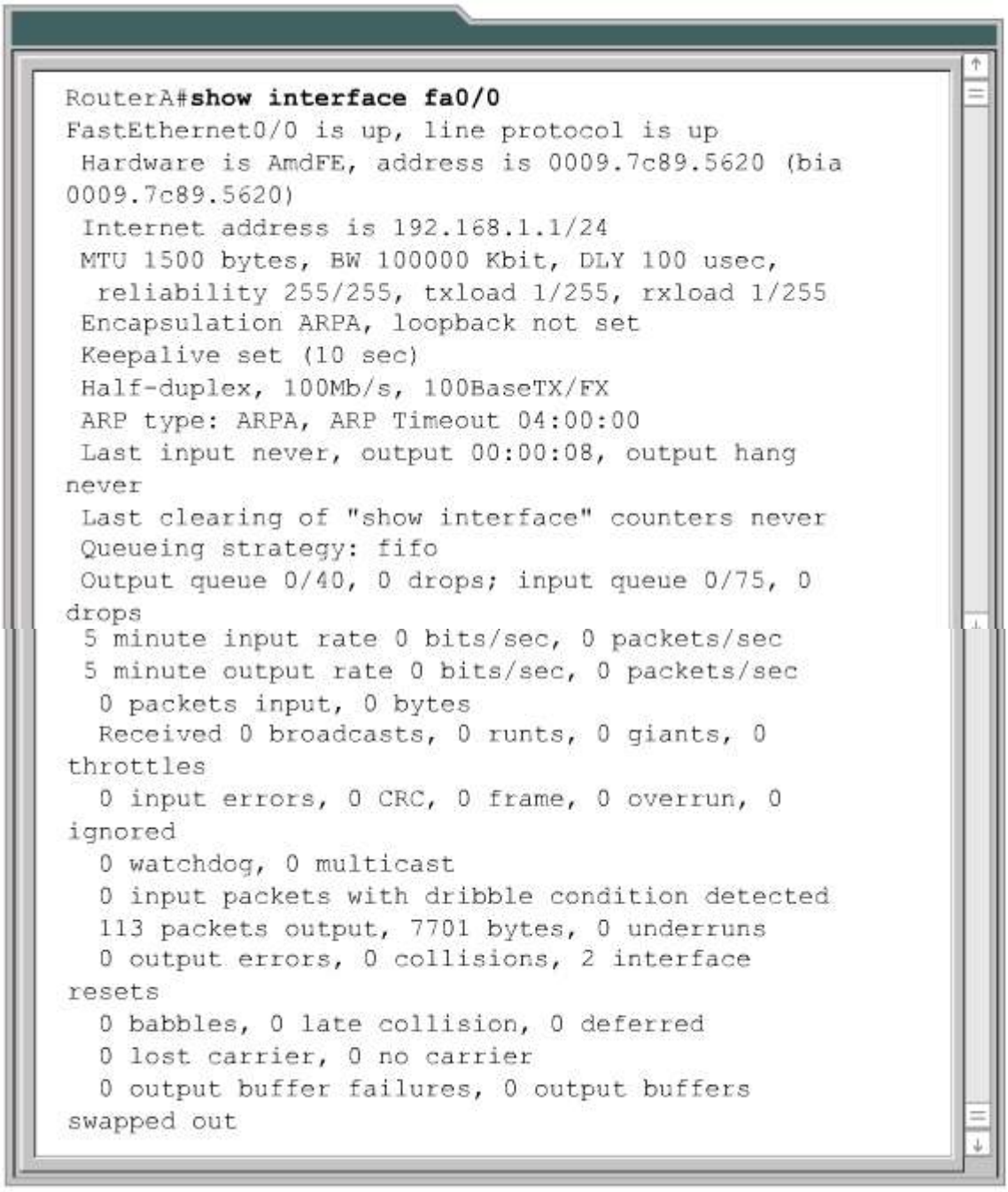
Pour vous assurer que le protocole IGRP a été correctement configuré, entrez la commande **show ip route** et recherchez les routes IGRP signalées par un “I”.

Des commandes supplémentaires permettent de vérifier la configuration IGRP, par exemple:

- **show interface***interface*
- **show running-config**
- **show running-config interface***interface*
- **show running-config | begin interface***interface*
- **show running-config | begin igrp**

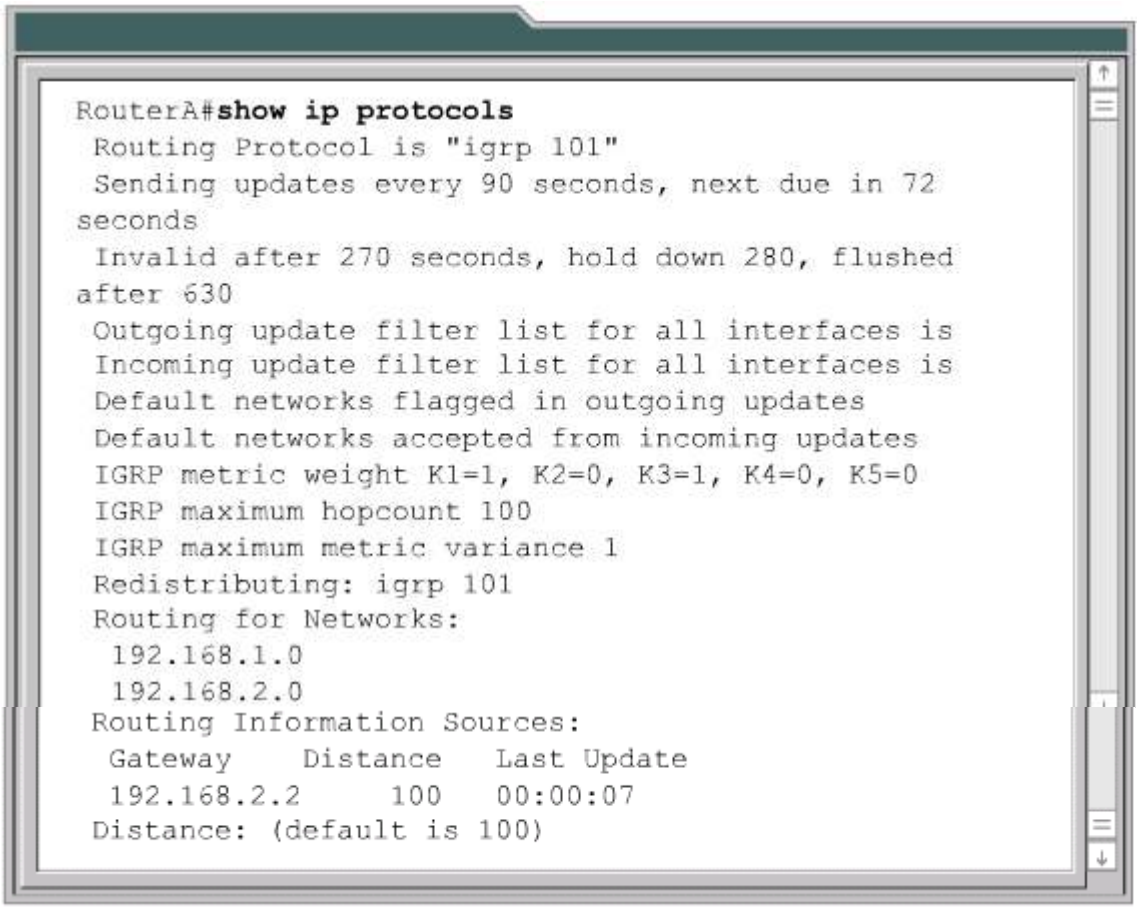
- **`show ip protocols`**

Pour vérifier si l'interface Ethernet est correctement configurée, entrez la commande **`show interface fa0/0`**. La figure 1 indique les informations générées.



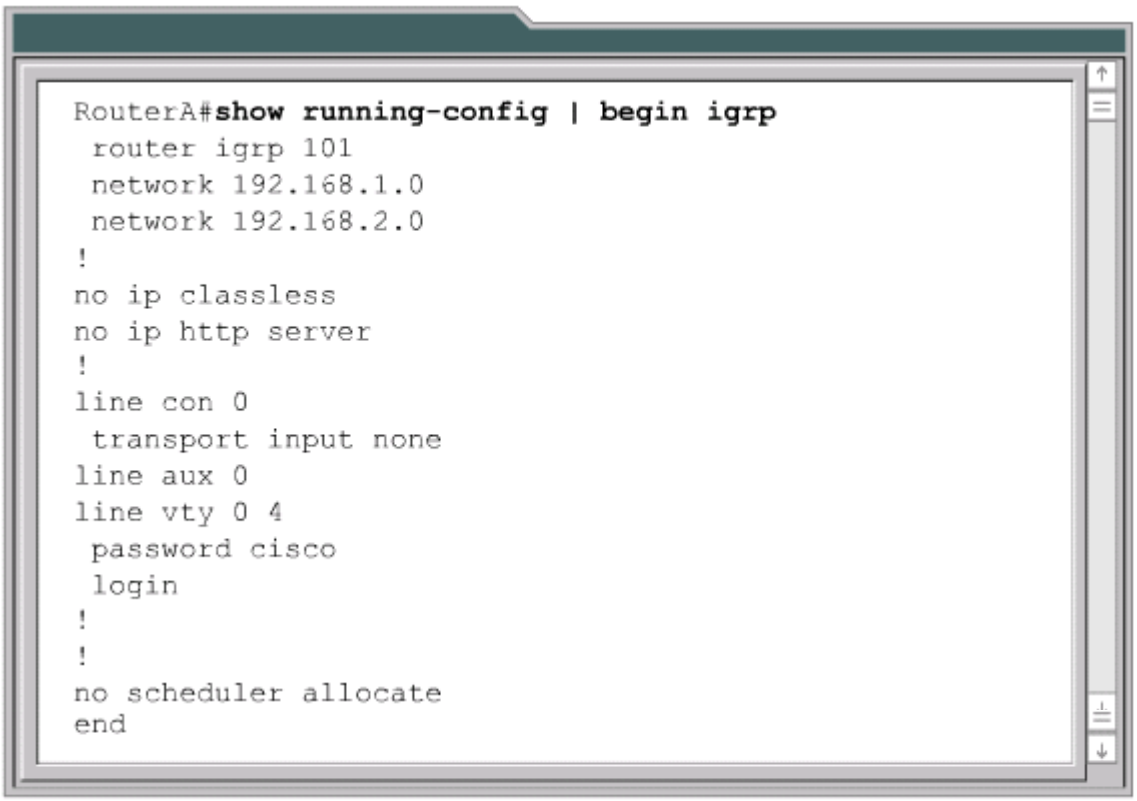
```
RouterA#show interface fa0/0
FastEthernet0/0 is up, line protocol is up
 Hardware is AmdFE, address is 0009.7c89.5620 (bia
0009.7c89.5620)
 Internet address is 192.168.1.1/24
 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
  reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Half-duplex, 100Mb/s, 100BaseTX/FX
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input never, output 00:00:08, output hang
never
 Last clearing of "show interface" counters never
 Queueing strategy: fifo
 Output queue 0/40, 0 drops; input queue 0/75, 0
drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0
throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0
ignored
    0 watchdog, 0 multicast
    0 input packets with dribble condition detected
    113 packets output, 7701 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface
resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers
swapped out
```

Pour savoir si le protocole IGRP est activé sur le routeur, entrez la commande **`show ip protocols`**. La figure 2 indique les informations générées.



```
RouterA#show ip protocols
 Routing Protocol is "igrp 101"
 Sending updates every 90 seconds, next due in 72
seconds
 Invalid after 270 seconds, hold down 280, flushed
after 630
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 IGRP maximum hopcount 100
 IGRP maximum metric variance 1
 Redistributing: igrp 101
 Routing for Networks:
  192.168.1.0
  192.168.2.0
 Routing Information Sources:
  Gateway    Distance    Last Update
  192.168.2.2      100    00:00:07
 Distance: (default is 100)
```

Les commandes présentées dans les figures 3 4 et 5 vérifient les paramètres réseau, l'adressage IP et les tables de routage.



```
RouterA#show running-config | begin igrp
 router igrp 101
 network 192.168.1.0
 network 192.168.2.0
!
no ip classless
no ip http server
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
!
no scheduler allocate
end
```

```
RouterA#show running-config interface fa0/0
Building configuration...

Current configuration:
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no ip directed-broadcast
end
```

```
RouterA#show ip route
Codes: C - connected, S - static, I - IGRP, R -
RIP, M - mobile, B - BGP
   D - EIGRP, EX - EIGRP external, O - OSPF, IA -
OSPF inter area
   N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
   E1 - OSPF external type 1, E2 - OSPF external
type 2, E - EGP
   i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS
level-2, ia - IS-IS inter area
   * - candidate default, U - per-user static
route, o - ODR
   P - periodic downloaded static route

Gateway of last resort is not set
C   192.168.1.0/24 is directly connected, Loopback0
C   192.168.2.0/24 is directly connected, Serial0/0
I   192.168.3.0/24 [100/80135] via 192.168.2.2,
00:01:00, Serial0/0
```

Activité de TP

Activité en ligne : Vérification de la configuration IGRP

Au cours de ce TP, les étudiants utiliseront des commandes show IOS pour vérifier le fonctionnement d'un routeur exécutant IGRP.

Activité de TP

Activité en ligne : IGRP

Au cours de ce TP, les étudiants configureront le routage dynamique entre les réseaux au moyen du protocole IGRP.

7.3 IGRP

7.3.8 Dépannage du protocole IGRP

La plupart des erreurs de configuration IGRP sont dues à une instruction réseau incorrecte, à des réseaux non contigus ou à un numéro de système autonome erroné.

Les commandes suivantes sont utiles lors du dépannage du protocole IGRP:

- **show ip protocols**
- **show ip route**
- **debug ip igrp events**
- **debug ip igrp transactions**
- **ping**
- **traceroute**

La figure 1 présente les informations générées par la commande **debug ip igrp events**.

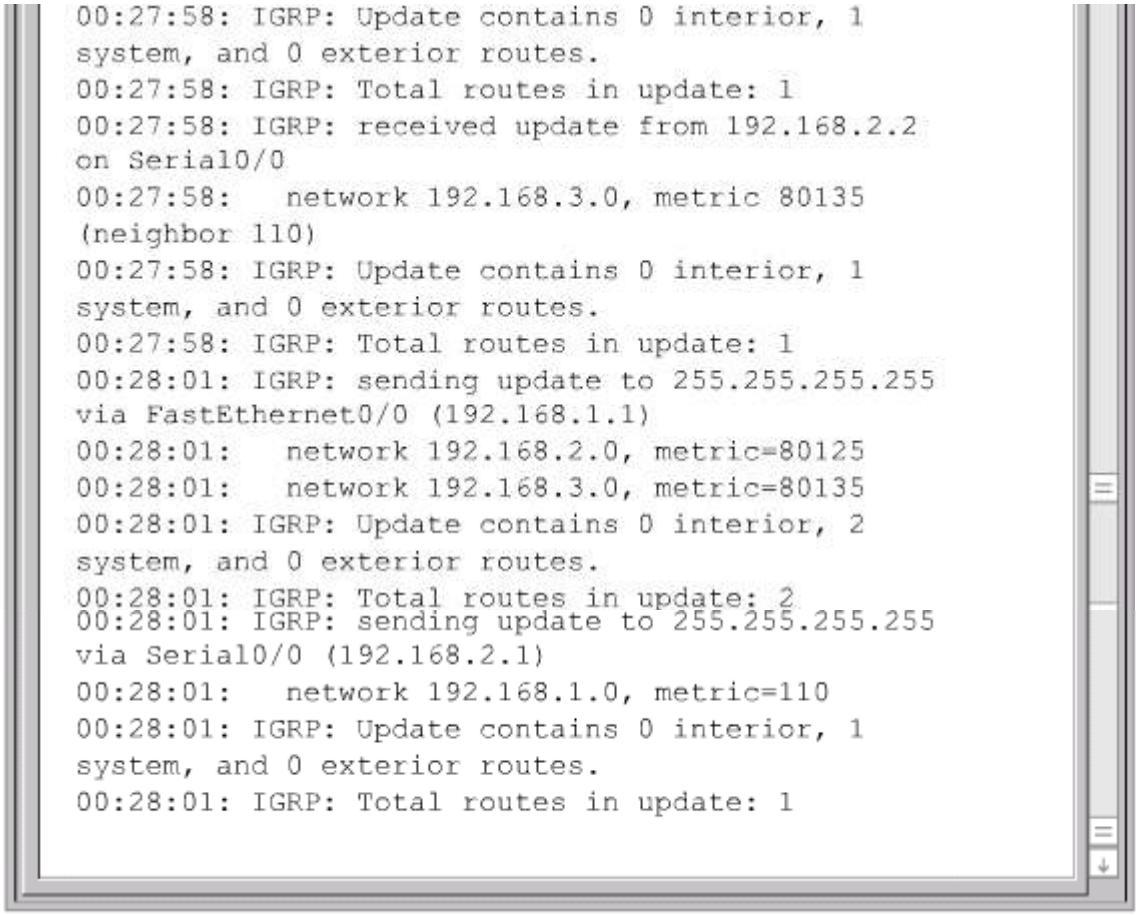
```
RouterA#debug ip igrp events
IGRP event debugging is on

00:21:38: IGRP: sending update to 255.255.255.255
via FastEthernet0/0 (192.168.1.1)
00:21:38: IGRP: Update contains 0 interior, 2
system, and 0 exterior routes.
00:21:38: IGRP: Total routes in update: 2
00:21:38: IGRP: sending update to 255.255.255.255
via Serial0/0 (192.168.2.1)
00:21:38: IGRP: Update contains 0 interior, 1
system, and 0 exterior routes.
00:21:38: IGRP: Total routes in update: 1
```

La figure 2 présente les informations générées par la commande **debug ip igrp transactions**.

```
RouterA#debug ip igrp transactions
IGRP protocol debugging is on

00:22:17: IGRP: received update from 192.168.2.2
on Serial0/0
00:22:17:   network 192.168.3.0, metric 80135
(neighbor 110)
00:23:07: IGRP: sending update to 255.255.255.255
via FastEthernet0/0 (192.168.1.1)
00:23:07:   network 192.168.2.0, metric=80125
00:23:07:   network 192.168.3.0, metric=80135
00:23:07: IGRP: sending update to 255.255.255.255
via Serial0/0 (192.168.2.1)
00:23:07:   network 192.168.1.0, metric=110
```

La commande a permis de détecter que le numéro de système autonome utilisé était erroné. La figure 3 affiche les informations générées une fois cette erreur corrigée.

```
RouterA(config)#no router igrp 102
RouterA(config)#router igrp 101
RouterA(config-router)#network 192.168.1.0
RouterA(config-router)#network 192.168.2.0

00:27:50: IGRP: broadcasting request on
FastEthernet0/0
00:27:50: IGRP: sending update to 255.255.255.255
via FastEthernet0/0 (192.168.1.1)
00:27:51: IGRP: Update contains 0 interior, 0
system, and 0 exterior routes.
00:27:51: IGRP: Total routes in update: 0 -
suppressing null update^Z
RouterA#
00:27:53: %SYS-5-CONFIG_I: Configured from console
by console
00:27:58: IGRP: received update from 192.168.2.2
on Serial0/0
00:27:58:   network 192.168.3.0, metric 80135
(neighbor 110)
00:27:58: IGRP: Update contains 0 interior, 1
system, and 0 exterior routes.
00:27:58: IGRP: Total routes in update: 1
00:27:58: IGRP: Total routes in update: 1
00:27:58: IGRP: sending update to 255.255.255.255
via FastEthernet0/0 (192.168.1.1)
00:27:58:   network 192.168.2.0, metric=80125
00:27:58:   network 192.168.3.0, metric=80135
00:27:58: IGRP: Update contains 0 interior, 2
system, and 0 exterior routes.
00:27:58: IGRP: Total routes in update: 2
00:27:58: IGRP: sending update to 255.255.255.255
via Serial0/0 (192.168.2.1)
```



Activité de TP

Exercice : Équilibrage de charge de coût différent avec IGRP

L'objectif de ce TP est d'observer l'équilibrage de charge de coût différent et de mettre au point les réseaux IGRP en utilisant des commandes de débogage avancées.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Mise à jour des informations de routage au moyen de protocoles à vecteur de distance
- Raisons de l'apparition de boucles de routage dans le cadre du routage à vecteur de distance
- Définition d'une valeur maximale pour éviter la métrique de mesure infinie
- Élimination des boucles de routage grâce à la solution split horizon
- Mode poison reverse
- Comment empêcher les boucles de routage avec les mises à jour déclenchées
- Comment éviter les boucles de routage grâce aux compteurs de retenue
- Comment empêcher les mises à jour du routage via une interface
- Équilibrage de charge sur plusieurs chemins
- Processus RIP
- Configuration du protocole RIP
- Utilisation de la commande **`ip classless`**
- Problèmes de configuration RIP fréquents
- Équilibrage de charge RIP
- Intégration des routes statiques avec le protocole RIP
- Vérification de la configuration RIP
- Caractéristiques du protocole IGRP
- Métriques du protocole IGRP
- Routes IGRP

- Caractéristiques de stabilité du protocole IGRP
- Configuration du protocole IGRP
- Migration de RIP vers IGRP
- Vérification de la configuration IGRP
- Dépannage du protocole IGRP

Résumé

- Les tables de routage sont mises à jour périodiquement, pendant que la topologie d'un réseau basé sur un protocole à vecteur de distance change.
- RIP est un protocole de routage à vecteur de distance.
- RIP a évolué au fil des années pour passer d'un protocole de routage par classes, RIP Version 1 (RIP v1), à un protocole de routage sans classe, RIP Version 2 (RIP v2).
- IGRP est un protocole de routage à vecteur de distance mis au point par Cisco.

Vue d'ensemble

Le protocole IP est limité car c'est un système dit d'acheminement au mieux. Il est dépourvu de mécanisme garantissant que les données sont acheminées, quels que soit les problèmes qu'il peut rencontrer sur le réseau. Les données peuvent ne pas atteindre leur destination pour une foule de raisons, telles que la panne matérielle, la configuration inappropriée ou l'inexactitude des informations de routage. Pour identifier ces défaillances, IP utilise le protocole ICMP (Internet Control Message Protocol) pour avertir l'émetteur des données d'une erreur dans le processus d'acheminement. Ce module décrit les divers types de messages d'erreur ICMP et certaines de leurs utilisations.

Parce qu'il n'intègre pas de mécanisme à cet effet, l'IP utilise ICMP pour envoyer et recevoir des messages d'erreur et de contrôle aux hôtes sur le réseau. Ce module est consacré aux messages de contrôle, qui sont des messages qui fournissent aux hôtes des informations ou des paramètres de configuration. La connaissance des messages de contrôle ICMP est une partie essentielle du dépannage des réseaux et une clé pour une compréhension approfondie des réseaux IP.

À la fin de ce module, les étudiants doivent être en mesure de:

- Décrire le protocole ICMP
- Décrire le format de message ICMP
- Identifier les types de messages d'erreur ICMP
- Identifier les causes potentielles des messages d'erreur ICMP spécifiques
- Décrire les messages de contrôle ICMP
- Identifier une variété de messages de contrôle ICMP utilisés aujourd'hui sur les réseaux
- Déterminer les causes des messages de contrôle ICMP

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
8.1	Vue d'ensemble des messages d'erreur TCP/IP
8.2	Messages de contrôle de la suite de protocoles TCP/IP

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
		• Utilisation du modèle OSI en tant que guide pour le dépannage systématique de réseau	• Évaluation du processus de communication TCP/IP et de ses protocoles associés

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
		• Utilisation du modèle OSI en tant que guide pour le dépannage systématique de réseau	

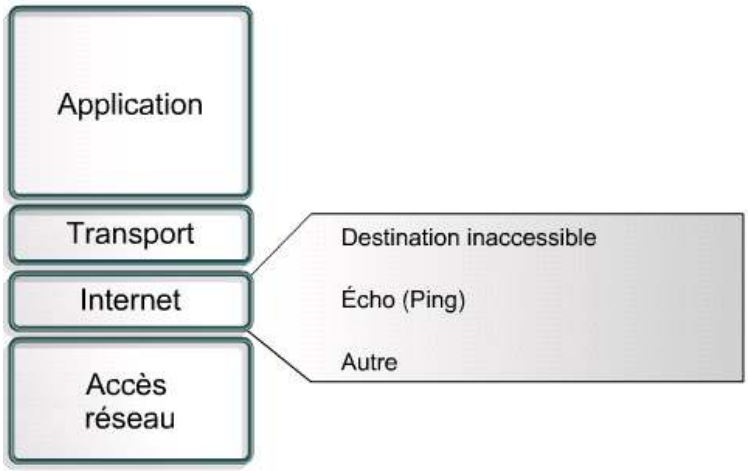
Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
• Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	• Utilisation des commandes intégrées à l'IOS pour analyser et signaler les problèmes sur le • Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	• Description de l'impact des protocoles associés à TCP/IP sur la communication des hôtes • Description du fonctionnement du protocole ICMP (Internet Control Message Protocol) et identification des raisons, des types et du format des messages d'erreur et de contrôle associés

8.1 Vue d'ensemble des messages d'erreur TCP/IP

8.1.1 ICMP (Internet Control Message Protocol

L'IP est une méthode peu fiable d'acheminement des données réseau. Il est connu comme un mécanisme d'acheminement au mieux. Il n'intègre aucun processus permettant de garantir que les données sont acheminées dans l'éventualité de problèmes de communication réseau. En cas de défaillance d'un équipement intermédiaire tel qu'un routeur, ou de déconnexion d'un équipement de destination du réseau, les données ne peuvent pas être acheminées. En outre, rien dans sa conception de base ne permet à l'IP de signaler à l'émetteur l'échec d'une transmission de données. Le protocole ICMP (Internet Control Message Protocol) est le composant de la pile de protocoles TCP/IP qui résout cette limitation de base d'IP. 1 ICMP ne compense pas les problèmes de manque de fiabilité d'IP. Si cela est nécessaire, la fiabilité doit être fournie par des protocoles de couche supérieure.

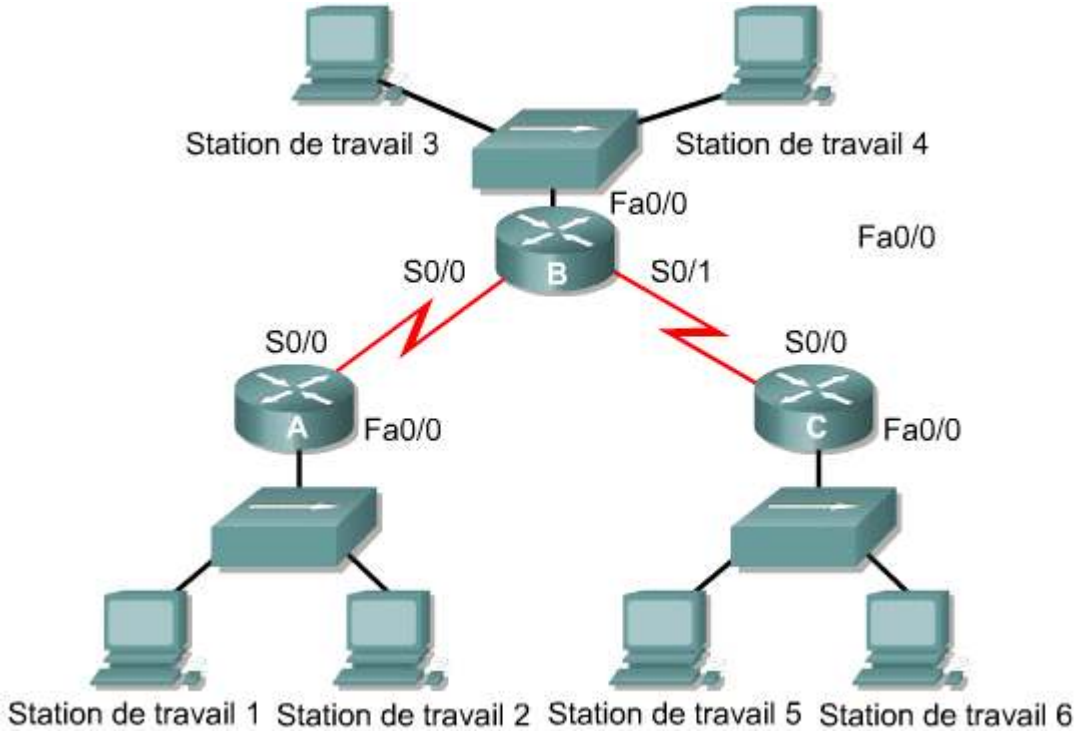


8.1 Vue d'ensemble des messages d'erreur TCP/IP

8.1.2 Signalement et correction des erreurs

L'ICMP est un protocole de signalement d'erreurs pour IP. Lorsque des erreurs de transmission de datagrammes se produisent, l'ICMP permet de les signaler à leur origine. Par exemple, si la station de travail 1 de la figure 1 envoie un datagramme à la station de travail, mais que l'interface Fa0/0 sur le routeur C s'arrête, le routeur C utilise ICMP pour envoyer un message à la station de travail 1 lui indiquant que le datagramme n'a pas pu être acheminé. L'ICMP ne corrige pas le problème réseau rencontré ; il ne fait que signaler le problème.

Lorsque le routeur C reçoit le datagramme de la station de travail 1, il connaît seulement les adresses IP d'origine et de destination du datagramme. Il ne connaît pas le chemin exact que le datagramme a emprunté pour aller jusqu'au routeur C. Par conséquent, le routeur C ne peut que signaler la panne à la station de travail 1, et aucun message ICMP n'est envoyé au routeur A et au routeur B. L'ICMP ne signale l'état du paquet transmis qu'à l'équipement d'origine. Il ne transmet pas aux routeurs des informations sur les changements survenus sur le réseau.



8.1 Vue d'ensemble des messages d'erreur TCP/IP

8.1.3 Acheminement de message ICMP

Les messages ICMP sont encapsulés dans des datagrammes de la même façon que toute autre donnée à l'aide d'IP. La figure 1 illustre l'encapsulation des données ICMP à l'intérieur d'un datagramme IP.

En-tête de trame	En-tête de datagramme	En-tête ICMP	Données ICMP
En-tête de trame	En-tête de datagramme	Zone de données du datagramme	
En-tête de trame	Zone de données de la		

Puisque les messages ICMP sont transmis de la même manière que les autres données, ils sont sujets aux mêmes problèmes d'acheminement. Cela engendre un scénario où les relevés d'erreur peuvent générer d'autres relevés, aggravant ainsi la congestion d'un réseau déjà mal en point. Pour cette raison, les erreurs créées par les messages ICMP ne génèrent pas leurs propres messages ICMP. Il est ainsi possible qu'une erreur de transmission de datagramme ne soit jamais signalée à l'émetteur des données.

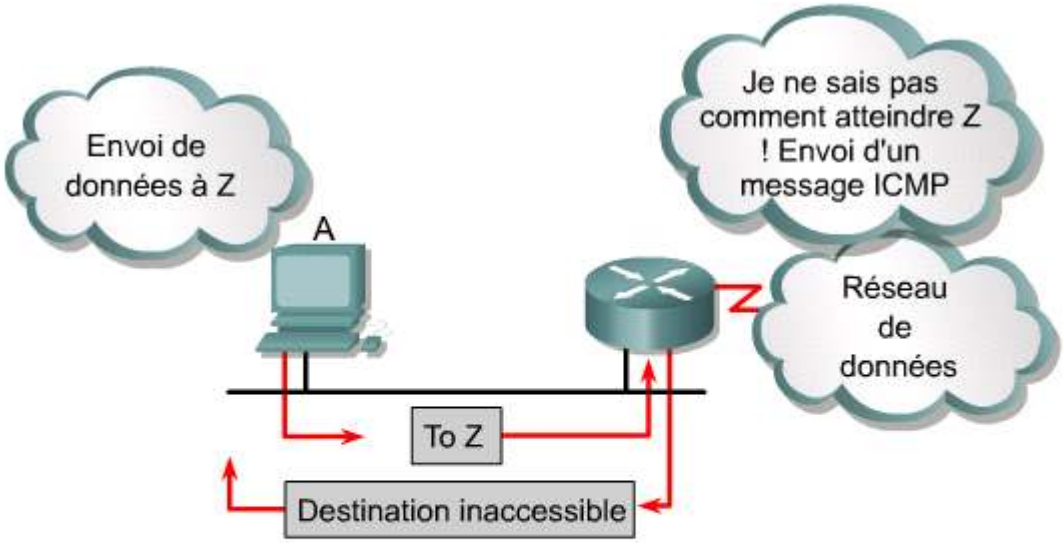
8.1 Vue d'ensemble des messages d'erreur TCP/IP

8.1.4 Réseaux inaccessibles

La communication réseau dépend de certaines conditions de base. D'abord, la pile de protocoles TCP/IP doit être correctement configurée sur les équipements émetteurs et récepteurs. Cela comprend l'installation du protocole TCP/IP et la configuration correcte de l'adresse IP et du masque de sous-réseau. Une passerelle par défaut doit également être configurée si les datagrammes doivent voyager à l'extérieur du réseau local. Deuxièmement, des équipements intermédiaires doivent être mis en place pour acheminer le datagramme de l'équipement d'origine et son réseau au réseau de destination. Les routeurs assurent cette fonction. Le protocole TCP/IP doit également être configuré de façon correcte sur les interfaces du routeur qui doit utiliser un protocole de routage approprié.

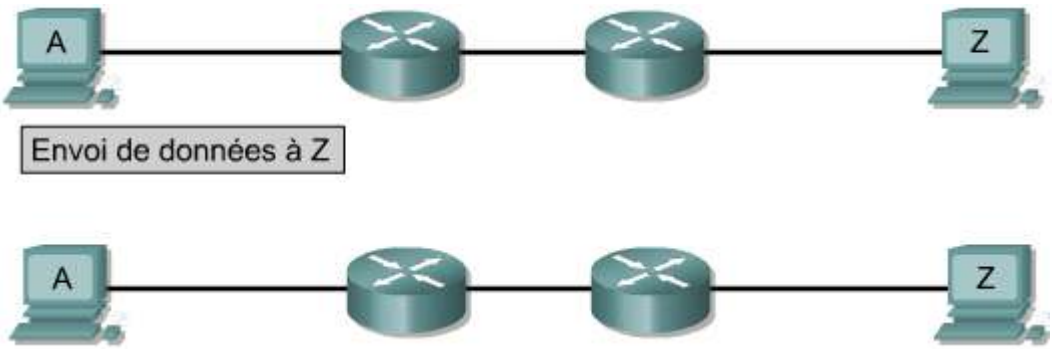
Si ces conditions ne sont pas remplies, la communication réseau ne peut avoir lieu. Par exemple, l'équipement émetteur peut adresser le datagramme à une adresse IP inexistante ou à un équipement de destination qui est déconnecté de son réseau. Les routeurs peuvent également être des points de défaillance si une interface de connexion est arrêtée ou s'ils ne disposent pas des informations nécessaires pour trouver le réseau de destination. S'il est impossible d'atteindre un réseau, on dit qu'il est inaccessible.

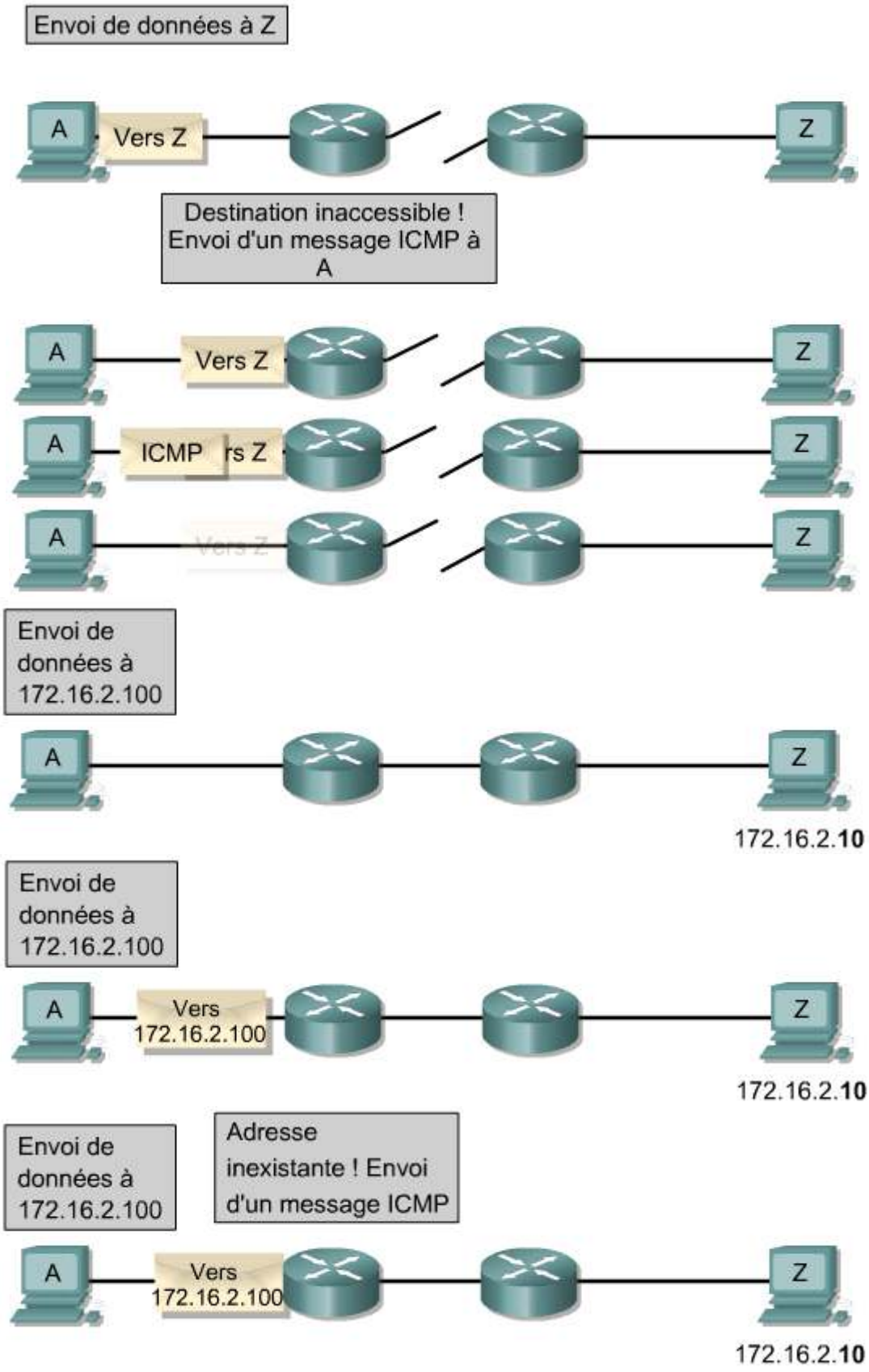
Les figures 1 et 2 illustrent un routeur incapable d'acheminer à sa destination finale un paquet qu'il a reçu. Le paquet est impossible à transmettre parce qu'aucun chemin connu ne mène à la destination. Il envoie donc à la source un message ICMP indiquant que l'hôte est inaccessible.

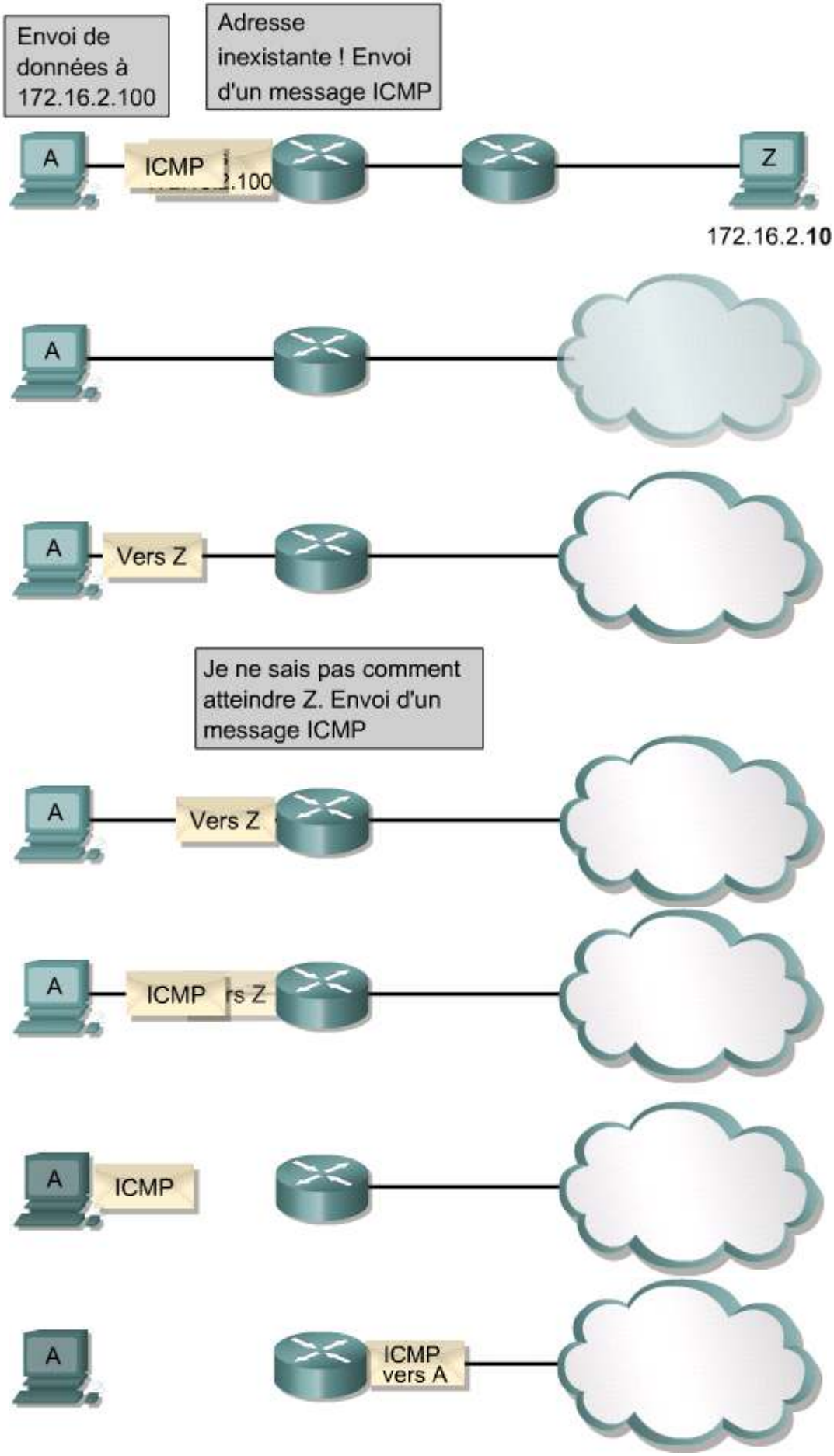


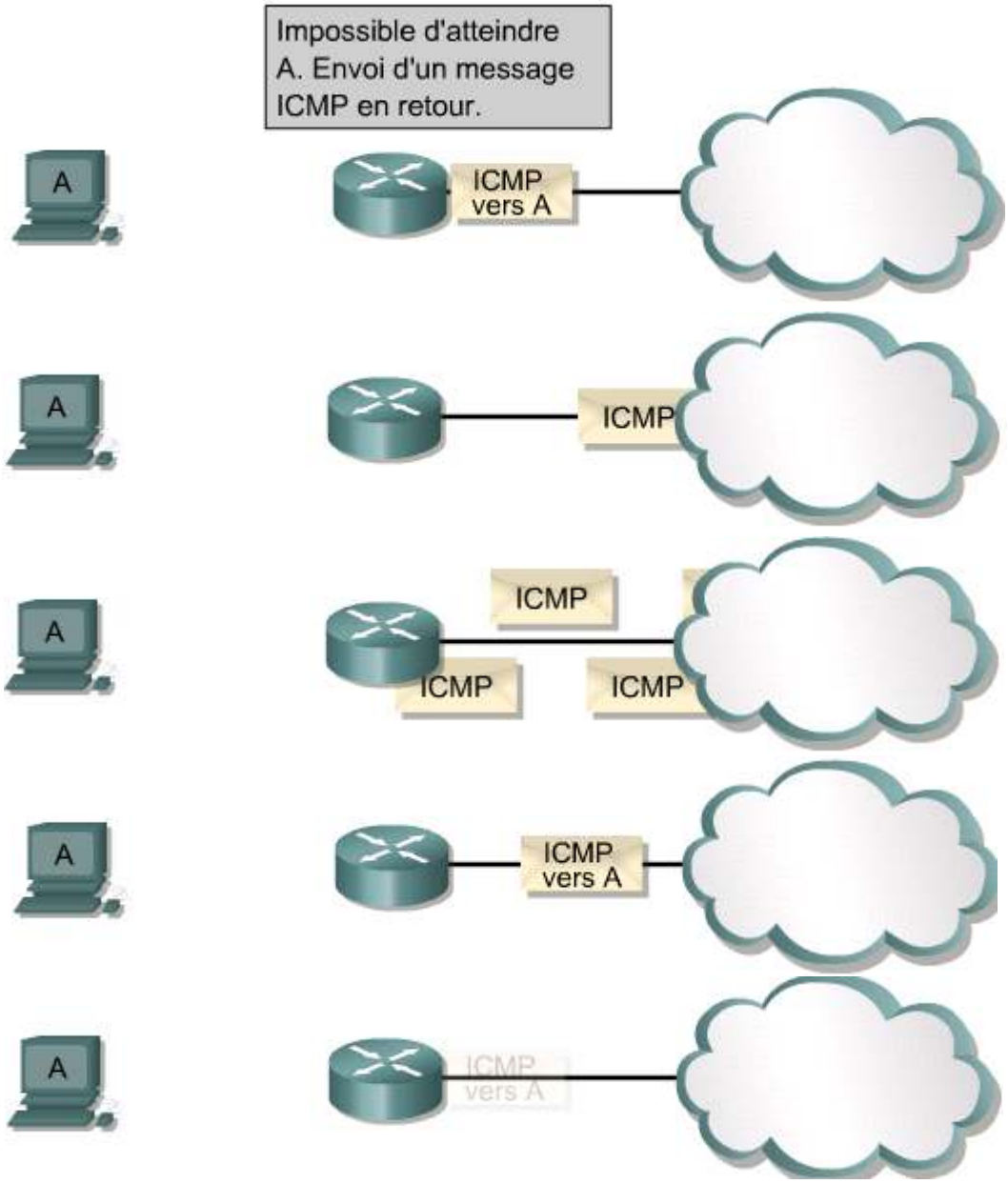
Un message ICMP " Destination inaccessible " est envoyé dans les cas suivants :

- Hôte ou port inaccessible
- Réseau inaccessible




Envoi de données à Z
A
Vers Z
Z
Destination inaccessible ! Envoi d'un message ICMP à A
A
Vers Z
Z
A
ICMP
rs Z
Z
A
Z
Envoi de données à 172.16.2.100
A
Z
172.16.2.10
Envoi de données à 172.16.2.100
A
Vers 172.16.2.100
Z
172.16.2.10
Envoi de données à 172.16.2.100
Adresse inexistante ! Envoi d'un message ICMP
A
Vers 172.16.2.100
Z
172.16.2.10

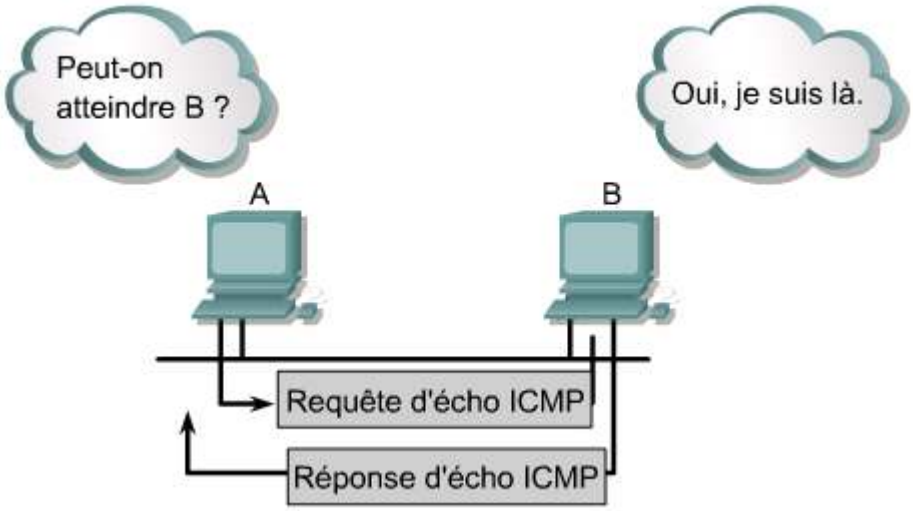

Envoi de données à 172.16.2.100
Adresse inexistante ! Envoi d'un message ICMP
A
ICMP
Z
172.16.2.10
A
A
Vers Z
Je ne sais pas comment atteindre Z. Envoi d'un message ICMP
A
Vers Z
A
ICMP
A
ICMP
A
ICMP vers A



8.1.5 Utilisation de requêtes ping pour tester l'accessibilité de la destination

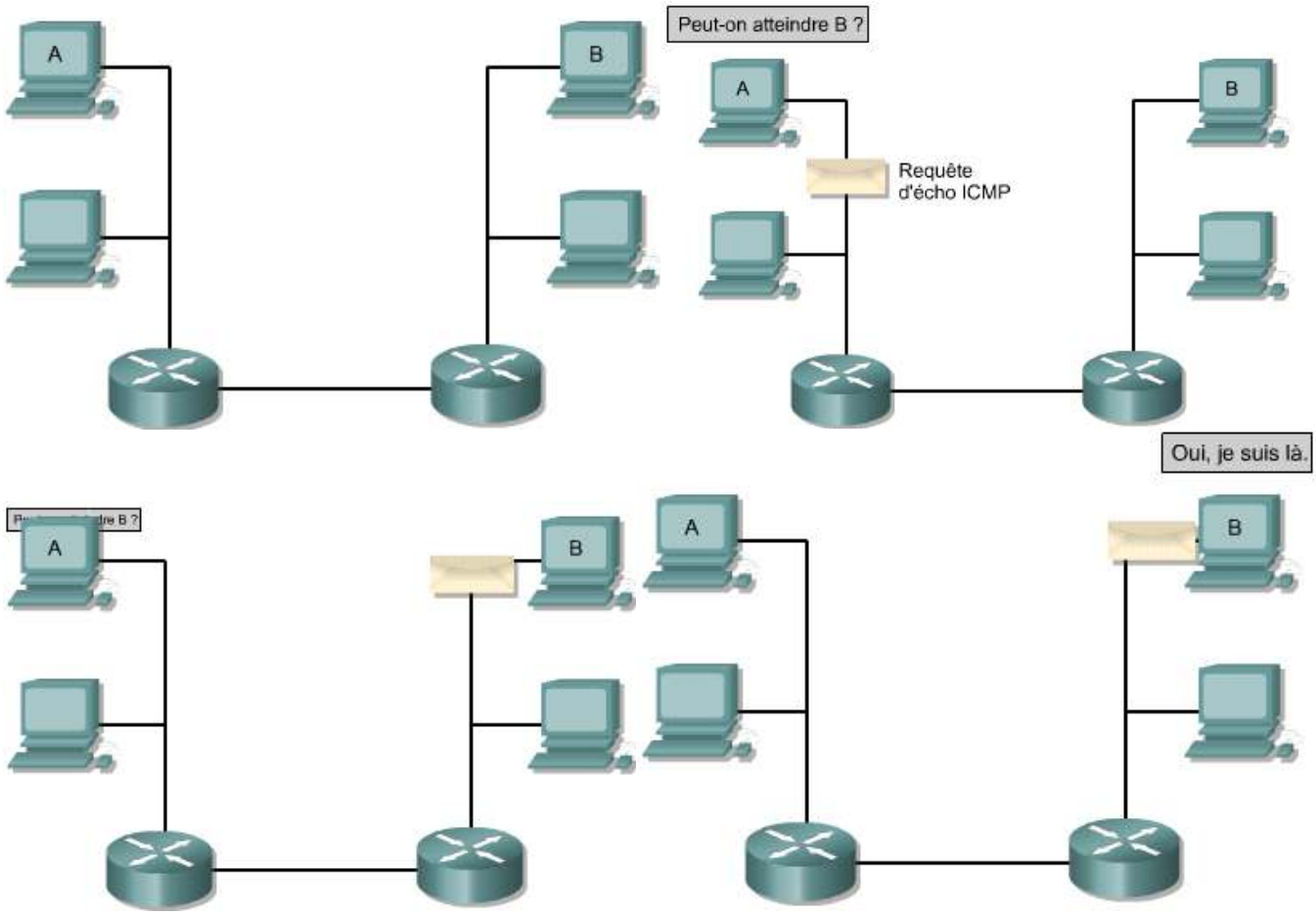
8.1.5 Utilisation de requêtes ping pour tester l'accessibilité de la destination

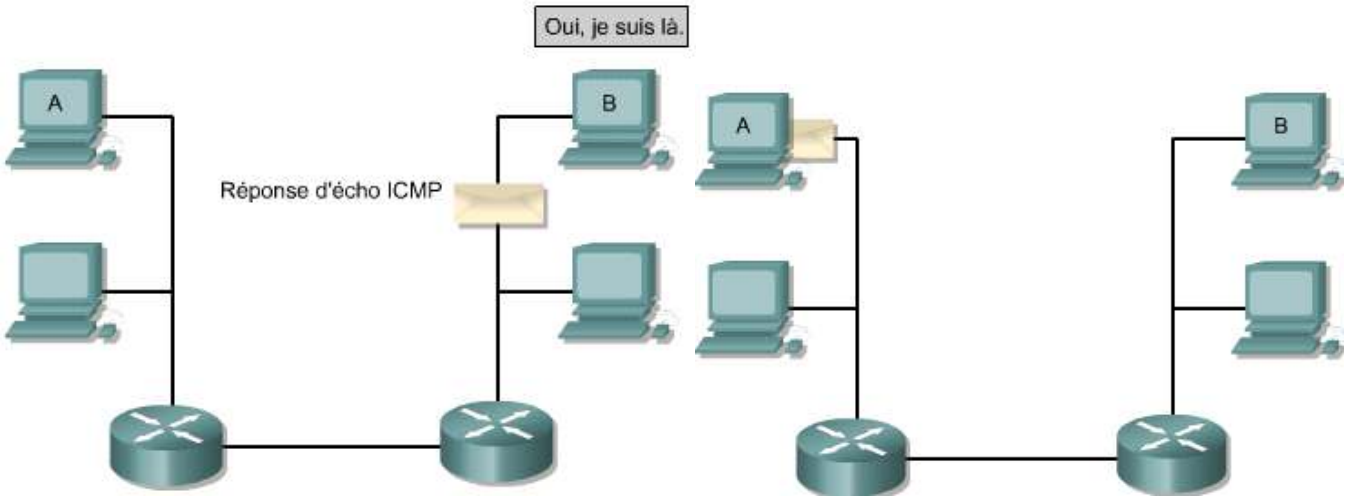
Le protocole ICMP peut être utilisé pour tester la disponibilité d'une destination particulière. La figure 1 illustre l'utilisation d'ICMP pour émettre un message de demande d'écho à l'équipement de destination. Si ce dernier reçoit la demande d'écho ICMP, il formule un message de réponse d'écho à retourner à l'origine de la demande d'écho. Si l'émetteur reçoit la réponse d'écho, cela confirme que l'équipement de destination est accessible via le protocole IP.



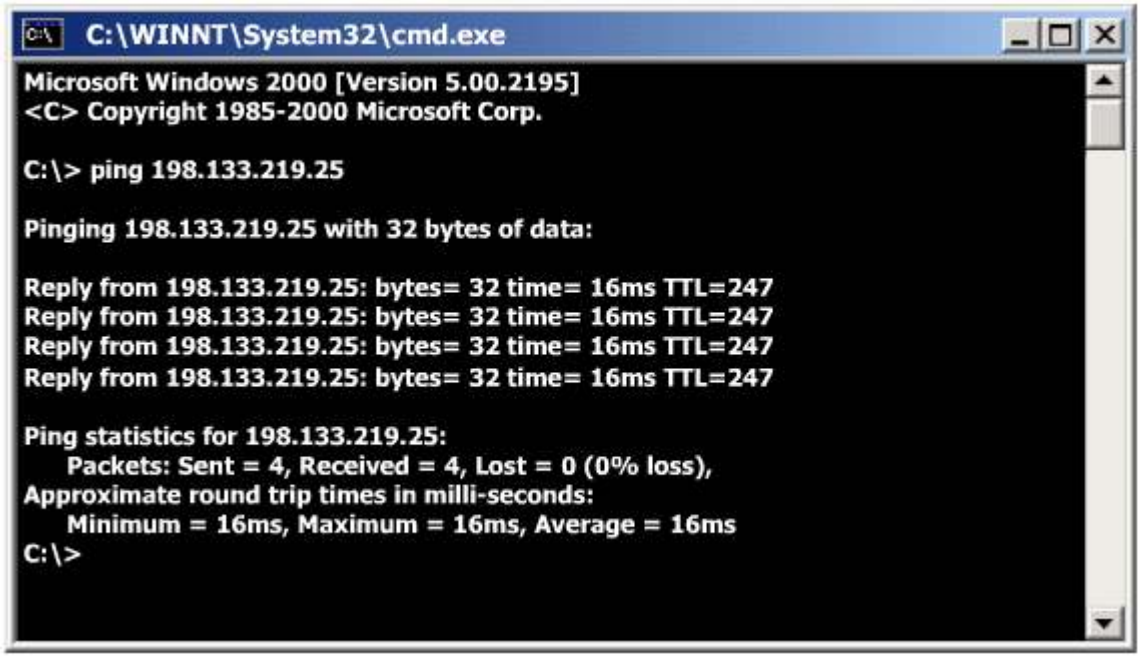
Trafic généré par la commande **ping**

Le message de demande d'écho est généralement lancé à l'aide de la commande **ping**, comme l'illustre la figure 2.





Dans cet exemple, la commande est utilisée avec l'adresse IP de l'équipement de destination. La commande peut aussi être entrée avec l'adresse IP de l'équipement de destination comme cela est illustré à la figure 3, en. Dans ces exemples, la commande **`ping`** émet quatre demandes d'écho et reçoit quatre réponses, confirmant la connectivité IP entre les deux équipements.

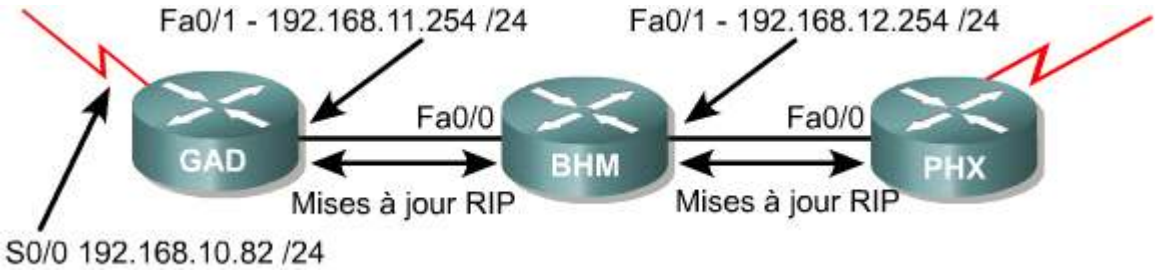


Comme cela est montré à la figure 3, le demande d'écho comprend une valeur de durée de vie (TTL, acronyme de time-to-live). La durée de vie est un champ contenu dans l'en tête du paquet IP qui permet de limiter la transmission des paquets. A chaque fois qu'un routeur transmet un paquet il décrémente la valeur TTL de un. Quand un routeur reçoit un paquet avec un TTL égal à 1, il ne transmet pas le paquet. Un message ICMP pourra être généré et envoyé à la machine émettrice et le paquet qui ne peut pas être délivré est détruit.

8.1.6 Détection de routes excessivement longues

8.1.6 Détection de routes excessivement longues

Des situations peuvent se produire où un datagramme est coincé dans une boucle, ne pouvant jamais atteindre sa destination. Ceci peut arriver si deux routeurs se renvoient continuellement le datagramme, pensant que l'autre est l'étape de saut suivant dans le chemin vers la destination. Quand plusieurs routeurs sont impliqués, un cycle de routage est créé. Dans un cycle de routage, un routeur envoie le datagramme vers le routeur de saut suivant et pense que celui-ci l'enverra vers la bonne destination. Le routeur de saut suivant route ensuite le datagramme vers le routeur suivant dans la boucle. Ceci est un exemple d'information de routage défectueuse. 1



Adresse de destination	Nombre de sauts	Adresse du saut suivant	Port
Table de routage partielle de GAD			
192.168.50.0 /24	14	192.168.10.83	S0/0
192.168.10.0 /24	0	---	S0/0
192.168.11.0 /24	0	---	Fa0/1
192.168.12.0 /24	1	192.168.11.253	Fa0/1
Table de routage partielle de BHM			
192.168.50.0 /24	15	192.168.11.254	Fa0/0
192.168.10.0 /24	1	192.168.11.254	Fa0/0
192.168.11.0 /24	0	---	Fa0/0
192.168.12.0 /24	0	---	Fa0/1
Table de routage partielle de PHX			
192.168.10.0 /24	2	192.168.12.254	Fa0/0
192.168.11.0 /24	1	192.168.12.254	Fa0/0
192.168.12.0 /24	0	---	Fa0/0

Les limitations du protocole de routage peuvent rendre les destinations inaccessibles. 1Par exemple, RIP limite la distance qu'un paquet peut parcourir. La limite de nombre de sauts du RIP est de 15, ce qui signifie qu'un réseau qui dépasse 15 sauts successifs ne pourra pas être appris à travers le protocole RIP.

Dans un cas comme dans l'autre, il existe une route excessivement longue. Que le chemin proprement dit reboucle sur lui-même ou comporte un nombre excessif de sauts, le paquet va dépasser le nombre de sauts maximum.

8.1 Vue d'ensemble des messages d'erreur TCP/IP

8.1.7 Messages d'écho

Comme n'importe quel type de paquet, les messages ICMP ont des formats spéciaux. Chaque type de message ICMP illustré à la Figure 1a ses propres caractéristiques uniques, mais tous les formats de messages ICMP commencent par ces trois champs:

- Type
- Code
- Checksum (somme de contrôle)

Le champ Type indique le type de message ICMP qui est envoyé. Le champ Code inclut des informations supplémentaires spécifiques au type de message. Le champ Checksum, comme dans d'autres types de paquets, permet de vérifier l'intégrité des données.

Types de message ICMP	
0	Réponse d'écho
3	Destination inaccessible
4	Épuisement de la source
5	Requête de redirection/modification
8	Requête d'écho
9	Annonce de routeur
10	Sélection de routeur
11	Dépassement du délai
12	Problème de paramètre
13	Demande d'horodatage
14	Réponse d'horodatage
15	Demande d'informations
16	Réponse à la demande d'informations
17	Demande de masque d'adresse
18	Réponse à la demande de masque d'adresse

La figure 2 illustre le format des messages de demande et de réponse d'écho ICMP. Les numéros de type et de code appropriés sont affichés pour chaque type de message. Les champs identificateur et numéro de séquence sont uniques aux messages de demande et de réponse d'écho. Ces champs sont utilisés pour établir la correspondance entre les réponses d'écho et la demande d'écho correspondante . Le champ données contient des informations supplémentaires qui peuvent faire partie du message de demande d'écho ou de réponse d'écho.

0	8	16	31
Type (0 ou 8)	Code (0)	Somme de contrôle	
Identifiant		Numéro de séquence	
Données facultatives			
. . .			

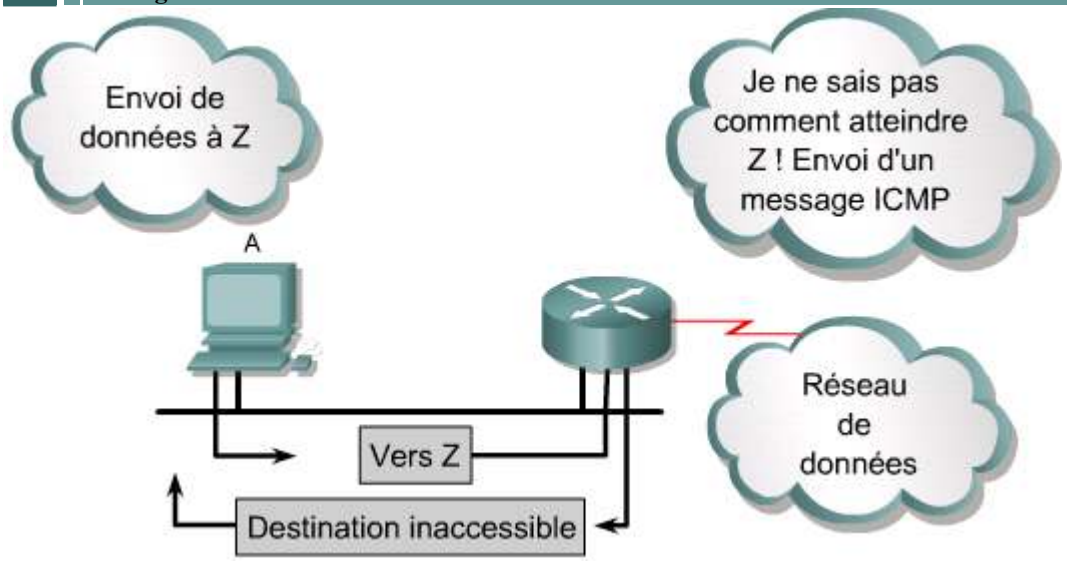
Activité de média interactive

Glisser-Positionner : Format de messsage d'écho ICMP

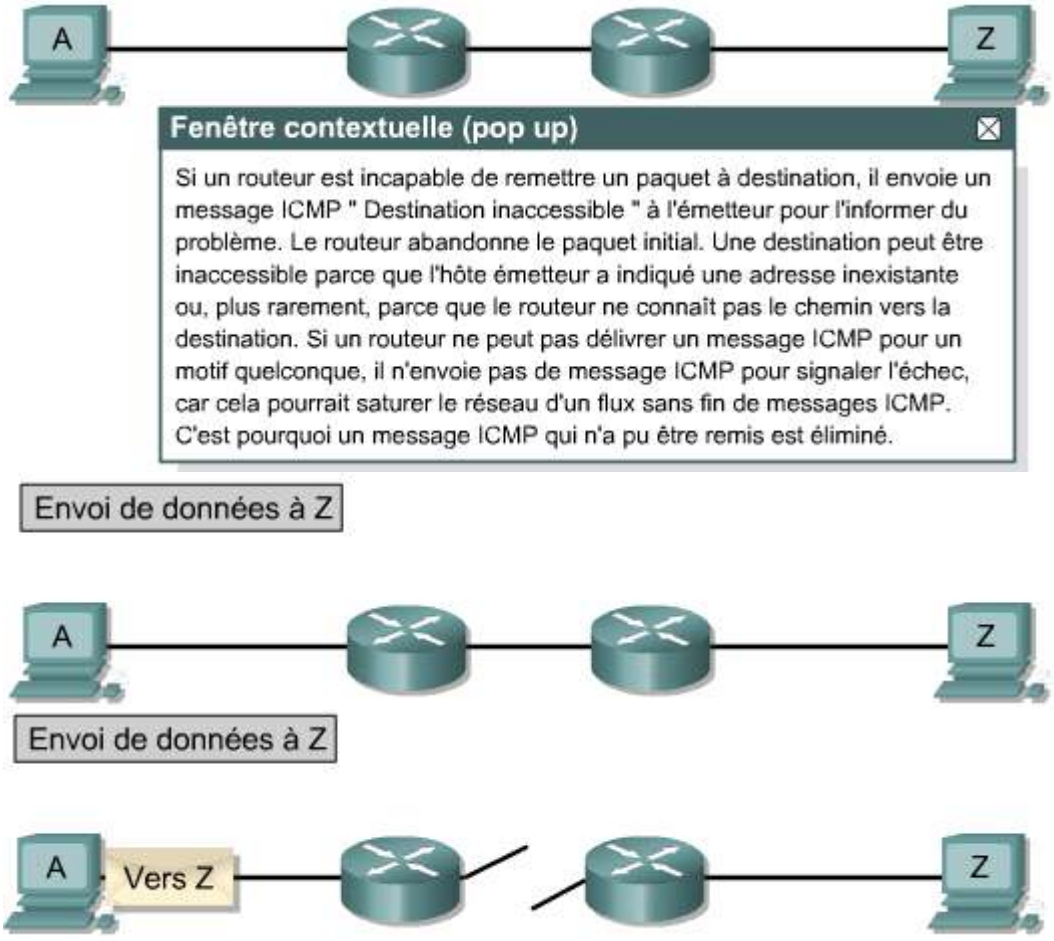
À la fin de cette activité, l'étudiant sera en mesure de comprendre le format du message d'écho ICMP.

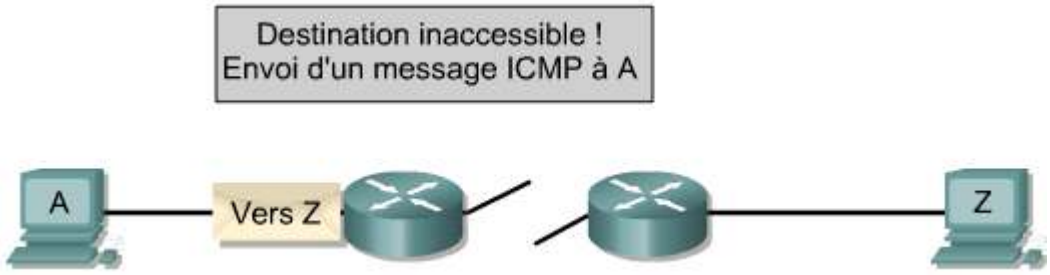
8.1 Vue d'ensemble des messages d'erreur TCP/IP

8.1.8 Message Destination inaccessible



Il n'est pas toujours possible d'acheminer des datagrammes à leur destination. 1 Les pannes matérielles, la configuration de protocole inappropriée, les arrêts d'interface et les informations de routage incorrectes sont autant de raison qui peuvent entraîner l'échec de l'acheminement. En pareil cas, ICMP retourne à l'émetteur un message «destination inaccessible» indiquant que le datagramme n'a pas pu être correctement acheminé. 2





La figure 3 montre un en-tête de message destination inaccessible d'ICMP. La valeur 3 dans le champ type indique qu'il s'agit d'un message destination inaccessible. La valeur du code indique la raison de la non transmission du paquet. La figure 3 a une valeur de code 0, indiquant que le réseau était inaccessible. La figure 4 illustre la signification de chaque valeur de code possible dans le message destination inaccessible.

0	8	16	31
Type (3)	Code (0-12)	Somme de contrôle	
Inutilisé (doit être zéro)			
En-tête Internet + 64 premiers bits du datagramme			
. . .			

0 = réseau inaccessible
1 = hôte inaccessible
2 = protocole inaccessible
3 = port inaccessible
4 = fragmentation nécessaire et DF défini
5 = échec de route source
6 = réseau de destination inconnu
7 = hôte de destination inconnu
8 = hôte source isolé
9 = communication avec le réseau de destination administrativement interdite
10 = communication avec l'hôte de destination administrativement interdite
11 = réseau inaccessible pour le type d'unité
12 = hôte inaccessible pour le type de service

Un message destination inaccessible peut également être envoyé lorsqu'il est nécessaire de fragmenter un paquet. C'est le cas en principe lorsqu'un datagramme est transmis d'un réseau Token-Ring à un réseau Ethernet. Si le datagramme ne permet pas la fragmentation, le paquet ne peut pas être transmis et le message destination inaccessible est envoyé. Des messages destination inaccessible peuvent également être générés si les services liés à l'IP tels que les services FTP ou les services Web ne sont pas disponibles. Pour dépanner de façon efficace un réseau IP, il est nécessaire de comprendre les diverses causes de l'apparition des messages destination inaccessible ICMP.

8.1 Vue d'ensemble des messages d'erreur TCP/IP

8.1.9 Signalement d'erreurs diverses

Certains types d'erreurs au niveau de l'en-tête peuvent empêcher les équipements qui traitent les datagrammes de les transmettre. Cette erreur n'est pas liée à l'état de l'hôte ou du réseau de destination, mais empêche quand même le traitement et l'acheminement du datagramme. En pareil cas, le datagramme est détruit et un message de problème de paramètre de type 12 ICMP est envoyé à l'origine du datagramme. La figure 1 illustre l'en-tête du message de problème de paramètre.

Cet en-tête inclut le champ pointeur. Lorsque la valeur de code est 0, le champ pointeur indique l'octet du datagramme qui a produit l'erreur.

0	8	16	31
Type (12)	Code (0-2)	Somme de contrôle	
Pointeur		Inutilisé (doit être zéro)	
En-tête Internet + 64 premiers bits du datagramme			
. . .			

8.2 Messages de contrôle TCP/IP Suite

8.2.1 Introduction aux messages de contrôle

L'ICMP (Internet Control Message Protocol) fait partie intégrante de la suite de protocoles TCP/IP. En fait, toutes les implémentations IP doivent inclure la prise en charge de ce problème. Cela pour de simples raisons. D'abord, puisque le protocole IP ne garantit pas l'acheminement, il n'intègre aucune méthode pour informer les hôtes de la survenue d'erreurs. Ensuite, l'IP n'intègre aucune méthode pour fournir aux hôtes des messages informatifs ou de contrôle. L'ICMP se charge de ces fonctions pour l'IP.

Contrairement aux messages d'erreur, les messages de contrôle ne résultent pas de paquets perdus ou de conditions d'erreurs qui se produisent lors de la transmission de paquets. À la place, ils sont utilisés pour informer les hôtes de conditions telles que la congestion du réseau ou de l'existence d'une meilleure passerelle jusqu'à un réseau distant. Les paquets ICMP utilisent les en têtes IP habituelles afin de pouvoir traverser plusieurs réseaux.

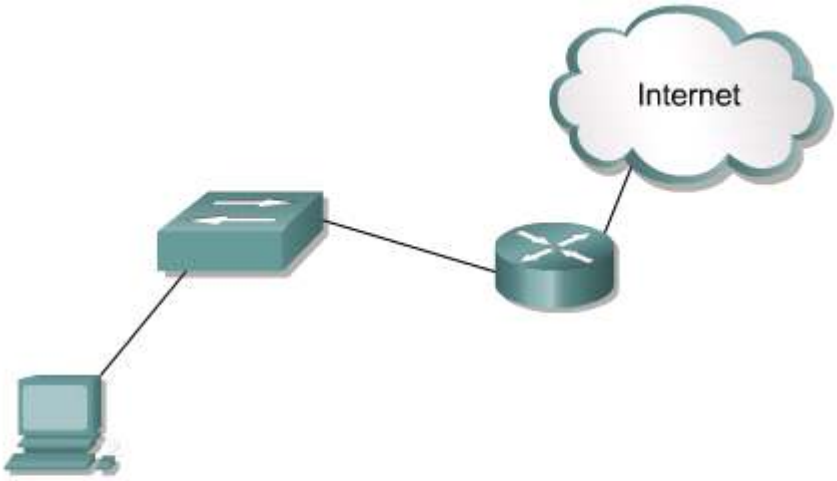
Plusieurs types de messages de contrôle sont utilisés par l'ICMP. Certains des plus communs sont illustrés à la figure 1. Nous en décrivons plusieurs dans cette section.

	Types de message ICMP
0	Réponse d'écho
3	Destination inaccessible
4	Épuisement de la source
5	Requête de redirection/modification
8	Requête d'écho
9	Annonce de routeur
10	Sélection de routeur
11	Dépassement du délai
12	Problème de paramètre
13	Demande d'horodatage
14	Réponse d'horodatage
15	Demande d'informations
16	Réponse à la demande d'informations
17	Demande de masque d'adresse
18	Réponse à la demande de masque d'adresse

8.2 Messages de contrôle TCP/IP Suite

8.2.2 Demandes de redirection/modification ICMP

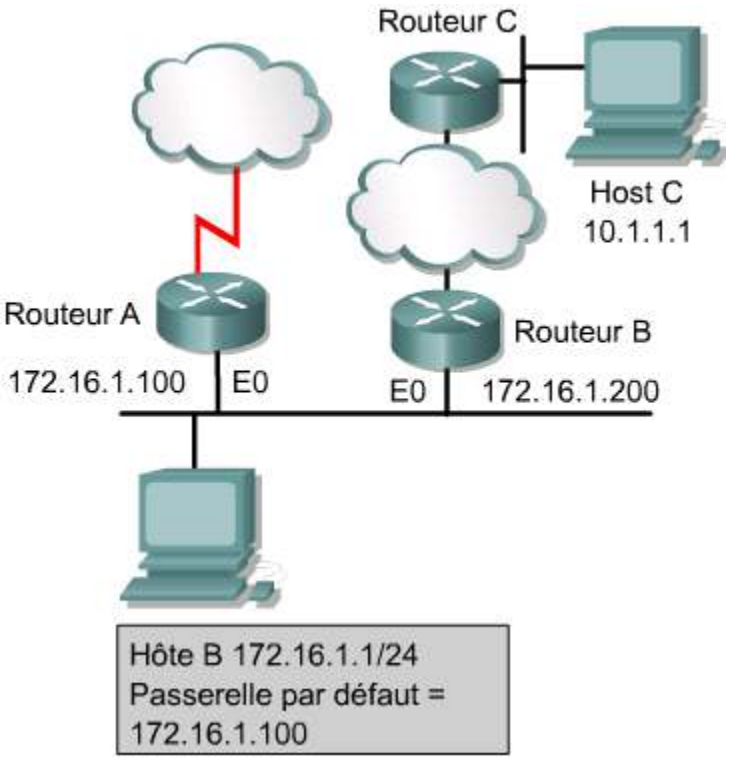
L'un des messages de contrôle les plus courants d'ICMP est la demande de redirection/modification. Ce type de message ne peut être émis que par une passerelle, qui est un terme couramment utilisé pour décrire un routeur. Tous les hôtes qui communiquent avec plusieurs réseaux IP doivent être configurés avec une passerelle par défaut. Cette passerelle est l'adresse d'un port de routeur connecté au même réseau que l'hôte. La figure 1 illustre un hôte connecté à un routeur qui a accès à Internet. Une fois configuré avec l'adresse IP Fa 0/0 comme passerelle par défaut, l'hôte B utilise cette adresse IP pour atteindre n'importe quel réseau non directement connecté à lui. Normalement, l'hôte B est connecté à une passerelle unique. Cependant, dans certaines cisconstances, un hôte se connecte à un segment qui comporte deux routeurs directement connectés, ou plus. Dans ce cas, la passerelle par défaut de l'hôte peut avoir besoin d'utiliser une demande de redirection/modification pour informer l'hôte du meilleur chemin vers un réseau donné.



Hôte B
Adresse IP : 192.168.12.4
Masque de sous-réseau 255.255.255.0
Passerelle par défaut : 192.168.12.1

Routeur A
FastEthernet 0/0 Adresse IP : 192.168.12.1
Masque de sous-réseau 255.255.255.0

La figure 2 illustre un réseau où des redirections ICMP pourraient être utilisées. L'hôte B envoie un paquet à l'hôte C sur le réseau 10.0.0.0/8. Puisque l'hôte B n'est pas directement connecté au même réseau, il transmet le paquet à sa passerelle par défaut, le routeur A. Le routeur A trouve la route appropriée vers le réseau 10.0.0.0/8 en consultant sa table de routage. Il détermine que le chemin vers le réseau emprunte la même interface d'où provient la demande de transmission du paquet. Il transmet le paquet et envoie une demande de redirection/modification à l'hôte B, lui indiquant d'utiliser le routeur B comme passerelle pour acheminer toutes les futures demandes au réseau 10.0.0.0/8.



Hôte B 172.16.1.1/24
Passerelle par défaut =
172.16.1.100

Les situations suivantes forceront les passerelles par défaut à envoyer des messages ICMP « redirect/change »

- L'interface via laquelle le paquet entre dans le routeur est la même que celle par laquelle il ressort.
- Le sous-réseau/réseau de l'adresse IP origine est identique à celui de l'adresse IP du saut suivant du paquet routé.
- Le datagramme n'est pas acheminé à l'origine.
- Le datagramme n'est pas acheminé à l'origine.

- La route de redirection n'est pas une autre redirection ICMP ou une route par défaut

La demande de redirection/modification ICMP utilise le format illustré à la figure 3. Elle a un code type ICMP de 5 et une valeur de code 0, 1, 2 ou 3. 4

0	8	16	31
Type (5)	Code (0-3)	Somme de contrôle	
Adresse Internet du routeur			
En-tête Internet + 64 premiers bits du datagramme			
. . .			

Valeur de code	Action requise
0	Datagrammes redirigés pour le réseau.
1	Datagrammes redirigés pour l'hôte.
2	Datagrammes redirigés pour le type de service et les réseaux.
3	Datagrammes redirigés pour le type de service et l'hôte.

Le champ Router Internet Address de la redirection ICMP est l'adresse IP qui serait utilisée comme passerelle par défaut pour un réseau particulier. Dans l'exemple de la Figure 2, la redirection ICMP envoyée du routeur A à l'hôte B comporterait un champ Router Internet Address de 172.16.1.200, qui est l'adresse IP de E0 sur le routeur B.

8.2 Messages de contrôle TCP/IP Suite

8.2.3 Synchronisation d'horloge et estimation du temps de transit

La suite de protocoles TCP/IP permet aux systèmes de se connecter les uns aux autres sur de vastes distances à travers plusieurs réseaux. Chacun de ces réseaux individuels fournit la synchronisation d'horloge à sa propre manière. Les hôtes de différents réseaux qui essaient de communiquer à l'aide de logiciels qui requièrent une synchronisation peuvent de ce fait rencontrer des problèmes. Le type de message d'horodatage ICMP est conçu pour éviter ce problème.

Le message de demande d'horodatage ICMP permet à un hôte de demander l'heure courante de l'hôte distant. L'hôte distant utilise un message de réponse d'horodatage ICMP pour répondre à la demande. 1

0	8	16	31
Type (13 ou 14)	Code (0)	Somme de contrôle	
Identifiant		Numéro de séquence	
Horodatage d'origine			
Horodatage de réception			
Horodatage de transmission			

Le champ type d'un message d'horodatage peut avoir la valeur 13 (demande d'horodatage) ou 14 (réponse d'horodatage). La valeur du champ code est toujours définie à 0 parce qu'aucun autre paramètre n'est disponible. La demande d'horodatage ICMP contient un horodatage de départ, qui est l'heure à laquelle l'hôte demandeur a envoyé la demande d'horodatage. L'horodatage de réception est l'heure à laquelle l'hôte de destination reçoit la demande d'horodatage ICMP. L'horodatage de transmission est renseigné juste avant que la réponse d'horodatage ICMP ne soit retournée. Les horodatages de départ, de réception et de transmission sont calculés en nombres de millisecondes écoulées depuis zéro heure, temps universel (UT).

Tous les messages de demande d'horodatage ICMP contiennent les horodatages de départ, de réception et de transmission. En utilisant ces trois horodatages, l'hôte peut déterminer le temps de transit sur le réseau en retranchant l'heure de départ et l'heure de réception. Il peut aussi déterminer la durée du transit pour le retour en retranchant l'heure de transmission à l'heure actuelle. Cela n'est toutefois qu'une estimation, car un temps de transit peut varier considérablement en fonction du trafic et de la congestion du réseau. L'hôte qui a émis la demande d'horodatage peut également estimer l'heure locale de l'ordinateur distant.

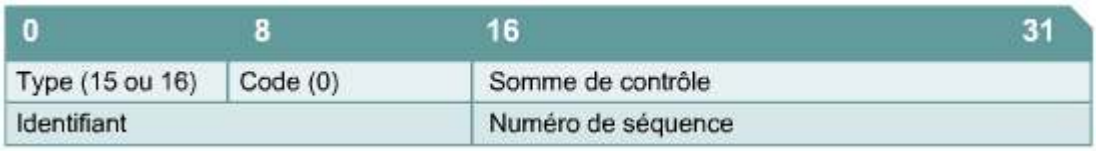
Bien que les messages d'horodatage ICMP permettent d'estimer facilement l'heure sur un ordinateur distant et la durée totale du transit sur le réseau, ils ne constituent pas le meilleur moyen d'obtenir ces informations. Pour cela, des protocoles plus

robustes tels que le NTP (Network Time Protocol), au niveau des couches supérieures de la pile de protocoles TCP/IP, effectuent la synchronisation d'horloge de façon bien plus fiable.

8.2 Messages de contrôle TCP/IP Suite

8.2.4 Format de messages de demande et de réponse

Les messages de demandes et de réponse d'informations ICMP étaient initialement conçus pour permettre à l'hôte de déterminer son numéro de réseau. La figure 1 illustre le format d'un message de demande et réponse d'information ICMP.



Deux codes de types sont disponibles dans ce message. Le type 15 correspond à un message de demande d'information et le type 16 à un message de réponse d'information. Ce type de message ICMP particulier est aujourd'hui considéré comme obsolète. D'autres protocoles tels que BOOTP, RARP (Reverse Address Resolution Protocol) et DHCP (Dynamic Host Configuration Protocol) sont à présent utilisés pour permettre aux hôtes d'obtenir leurs numéros de réseau.

8.2 Messages de contrôle TCP/IP Suite

8.2.5 Requêtes de masque d'adresse

Lorsqu'un administrateur réseau emploie le processus de sous-réseau pour diviser une adresse IP principale en plusieurs sous-réseaux, un nouveau sous-réseau est crée. Ce nouveau masque de sous-réseau est crucial pour l'identification des bits de réseau, de sous-réseau et d'hôtes dans une adresse IP. Si un hôte ne connaît pas le masque de sous-réseau, il peut envoyer une demande de masque d'adresse au routeur local. Si l'adresse du routeur est connue, cette demande peut être envoyée directement au routeur. Sinon, la demande est diffusée. Quand le routeur reçoit la demande, il retourne une réponse de masque d'adresse. Cette adresse identifie le masque de sous-réseau correct. Supposons par exemple qu'un hôte se trouve sur un réseau de classe B et possède l'adresse IP 172.16.5.2. Cet hôte ne connaît pas le masque de sous-réseau, donc il diffuse une demande de masque d'adresse :

```
Source address: 172.16.5.2
Destination address: 255.255.255.255
Protocol:  ICMP = 1
Type: Address Mask Request = AM1
Code: 0
Mask: 255.255.255.0
```

Le routeur local, 172.16.5.1, reçoit ce broadcast. Il adresse en retour la réponse de masque d'adresse suivante :

```
Source address: 172.16.5.1
Destination address: 172.16.5.2
Protocol: ICMP = 1
Type: Address Mask Reply = AM2
Code: 0
Mask: 255.255.255.0
```

Le format de trame de la demande et de la réponse de masque d'adresse est illustré à la figure 1. La figure 2 présente les descriptions de chaque champ du message de demande de masque d'adresse. Notez que le même format de trame pour la demande et la réponse. Cependant, le numéro de type 17 est attribué à la demande et 18 à la réponse.

0	8	16	31
Type (17 ou 18)	Code (0)	Somme de contrôle	
Identifiant		Numéro de séquence	
Masque d'adresse			
. . .			

Champs IP	
Adresses	Pour créer un message de réponse à une demande de masque d'adresse, l'adresse source de la demande devient l'adresse de destination de la réponse, et l'adresse source de la réponse correspond à l'adresse de l'unité ayant répondu. Le type de code changé est AM2 la valeur d'adresse de masque insérée dans le champ de masque d'adresse, et la somme de contrôle recalculée. Cependant, si l'adresse source dans le message de requête est zéro, alors l'adresse de destination pour le message de réponse devrait indiquer une adresse de broadcast.

Type 17	Message " Demande de masque d'adresse "
Type 18	Message " Réponse à la demande de masque d'adresse "
Code 0	Message " Demande de masque d'adresse "
Code 0	Message " Réponse à la demande de masque d'adresse "
Somme de contrôle	La somme de contrôle correspond au complément à un sur 16 bits de la somme des compléments à un des messages ICMP, à partir du type ICMP. Pour calculer la somme de contrôle, le champ correspondant doit être fixé à zéro. Cette somme de contrôle peut être remplacée ultérieurement.
Identifiant	Identifiant pouvant être utilisé pour mettre en correspondance les demandes et les réponses ; peut être égal à zéro.
Numéro de séquence	Séquence pouvant être utilisée pour mettre en correspondance lesdeman
Masque d'adresse	Masque sur 32 bits. Une passerelle recevant une demande de masque d'adresse doit la renvoyer avec le champ de masque d'adresse défini sur le masque 32 bits des bits identifiant le sous-réseau et le réseau, pour le sous-réseau sur lequel la demande a été reçue. Si l'hôte demandeur ne connaît pas sa propre adresse IP, il peut indiquer zéro dans le champ source ; la reponse est ensuite diffusée. Toutefois, cette approche doit être évitée si possible, car elle accroît la charge de broadcast superflue sur le réseau. Même lorsque les réponses sont diffusées, étant donné qu'il n'existe qu'un seul masque d'adresse possible pour un sous-réseau, il n'est pas nécessaire de mettre en correspondance les demandes et les réponses. Les champs Identifiant et Numéro de séquence peuvent être ignorés. Le type AM1 peut être reçu à partir d'une passerelle ou d'un hôte. Le type AM2 peut être reçu à partir d'une passerelle ou d'un hôte servant de passerelle.

8.2 Messages de contrôle TCP/IP Suite

8.2.6 Message de détection de routeur

Lorsqu'un hôte démarre sur le réseau et qu'il n'a pas été configuré manuellement avec une passerelle par défaut, il peut prendre connaissance des routeurs disponibles au travers du processus de détection de routeur. Ce processus débute avec l'envoi par l'hôte d'un message de sollicitation de routeur à tous les routeurs, en utilisant l'adresse multicast 224.0.0.2 comme adresse de destination. La figure 1 présente le message de détection de routeur ICMP. Ce message peut également être diffusé pour inclure des routeurs pouvant ne pas être configurés pour la diffusion multicast. Si un message de détection

de routeur est envoyé à un routeur qui ne prend pas en charge le processus de détection, la sollicitation restera sans réponse.

0	8	16	31
Type (9)	Code (0)	Somme de contrôle	
Nombre d'adresses	Taille d'entrée d'adresse	Durée de vie	
Adresse du routeur 1			
Niveau de préférences 1			
Adresse du routeur 2			
Niveau de préférences 2			

Lorsqu'un routeur qui prend en charge le processus de détection reçoit le message de détection de routeur, il retourne une annonce de routeur. Le format de trame d'annonce de routeur est illustré à la figure 1et une explication de chaque champ est donnée à la figure 2.

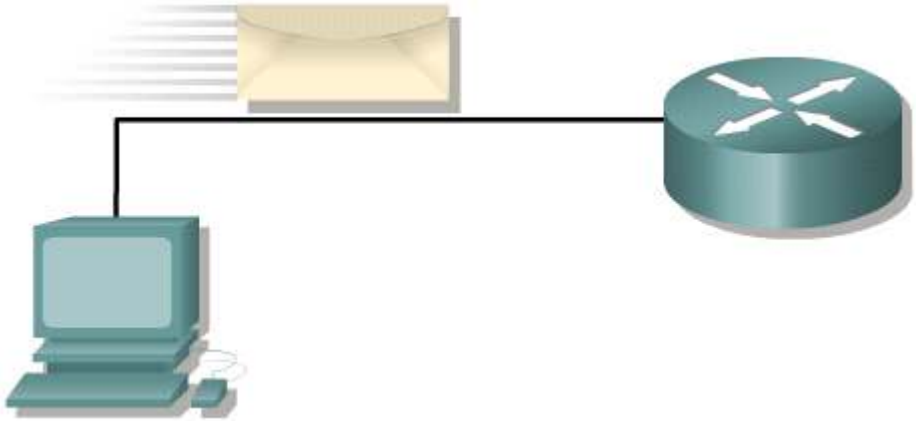
Champs IP	
Adresse source	Adresse IP appartenant à l'interface à partir de laquelle ce message est envoyé.
Adresse de destination	Adresse d'annonce configurée ou adresse IP d'un hôte voisin.
Durée de vie	1 si l'adresse de destination est une adresse multicast IP ; sinon, au moins 1.

ICMP	
Type	9
Code	0
Somme de contrôle	Complément à un sur 16 bits de la somme des compléments à un du message ICMP, à partir du type ICMP. Pour calculer la somme de contrôle, le champ correspondant est fixé à zéro.
Nombre d'adresses	Nombre d'adresses de routeur annoncées dans ce message.
Taille d'entrée	Nombres de mots de 32 bits pour chaque adresse de routeur (2 dans la version du protocole décrit ici).
Durée de vie	Nombre maximum de secondes pendant lesquelles les adresses du routeur sont considérées comme valides.
Adresse de routeur[i] i = 1..Nombre d'adresses	Adresse(s) IP du routeur expéditeur sur l'interface à partir de laquelle ce message est envoyé.
Niveau de préférences[i] i = 1..Nombre	Niveau de préférence de chaque adresse de routeur[i] comme adresse de routeur par défaut, par rapport aux autres adresses de routeur du même sous-réseau. Valeur de complément à deux signée ; les valeurs supérieures indiquent un niveau de préférence supérieur.

8.2 Messages de contrôle TCP/IP Suite

8.2.7 Message de sollicitation de routeur

Un hôte génère un message de sollicitation de routeur ICMP en réponse à une passerelle par défaut manquante. 1Ce message est envoyé via multicast et c'est la première étape du processus de détection du routeur. Un routeur local répondra avec une annonce identifiant la passerelle par défaut pour l'hôte local. La figure 2identifie le format de trame et la figure 3présente une explication de chaque champ.



0	8	16	31
Type (10)	Code (0)	Somme de contrôle	
Réservé			

Champs IP	
Adresse source	Adresse IP appartenant à l'interface à partir de laquelle ce message est envoyé, ou 0.
Adresse de destination	Adresse de sollicitation configurée
Durée de vie	Si l'adresse de destination est une adresse IP multicast; autrement, au moins 1

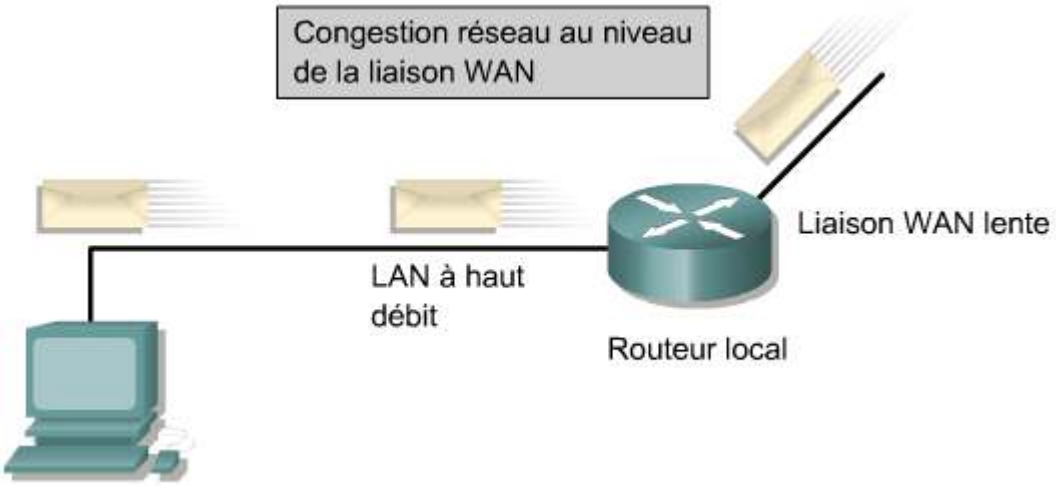
Champs ICMP	
Type	10
Code	0
Somme de contrôle	Complément à un sur 16 bits de la somme des compléments à un du message ICMP, à partir du type ICMP. Pour calculer la somme de contrôle, le champ correspondant est fixé à zéro.
Réservé	Envoyé à 0; ignoré à la réception

8.2 Messages de contrôle TCP/IP Suite

8.2.8 Messages de congestion et de contrôle de flux

Si plusieurs ordinateurs tentent d'accéder simultanément à la même destination, l'ordinateur de destination risque d'être submergé. La congestion peut également se produire lorsque le trafic d'un réseau LAN rapide accède à une connexion WAN plus lente. Une trop forte congestion entraîne un abandon de paquets. Les messages d'épuisement de la source ICMP sont utilisés pour limiter la perte de données. Ce message demande à l'émetteur de réduire le débit de transmission des paquets. Dans la plupart des cas, la congestion s'atténue en peu de temps, et l'origine peut augmenter le débit progressivement tant qu'elle ne reçoit pas d'autres messages d'épuisement de la source. La plupart des routeurs Cisco n'envoient pas ce type de message par défaut, car il peut lui-même contribuer à la congestion du réseau.

C'est dans le contexte des très petits bureaux/bureaux à domicile que les messages d'épuisement de la source ICMP peuvent s'avérer efficaces. Un tel réseau pourrait consister de quatre ordinateurs interconnectés à l'aide d'un câble CAT-5 et se partageant une connexion Internet (ICS) sur un modem 56K. Il est évident que la bande passante à 10 Mbps du réseau LAN des très petits bureaux/bureaux à domicile peut rapidement submerger la bande passante de 56 K de la liaison WAN, entraînant ainsi la perte de données et les retransmissions. L'hôte d'interconnexion peut utiliser un message ICMP « source quench » pour demander que les autres hôtes réduisent leur vitesse de transmission. Ceci permet de réduire la perte de données. La figure 1 illustre un réseau où la congestion sur la liaison WAN pourrait entraîner des problèmes de communication.



Résumé

La compréhension des points clés suivants devrait être acquise:

- L'IP est une méthode d'acheminement au mieux qui utilise des messages ICMP pour signaler à l'émetteur que les données n'ont pas atteint leur destination
- Les messages de demande et de réponse d'écho ICMP permettent à l'administrateur réseau de tester la connectivité IP en vue du dépannage
- Les messages ICMP sont transmis à l'aide du protocole IP ; leur acheminement n'est donc pas fiable
- Les paquets ICMP possèdent leurs propres informations d'en-tête spéciales, avec un champ type et un champ code
- Identification des causes potentielles des messages d'erreur ICMP spécifiques
- Les fonctions des messages de contrôle ICMP
- Les demandes de redirection/modification ICMP
- Les messages de synchronisation d'horloge et d'estimation du temps de transit ICMP
- Les messages de demande et de réponse d'information ICMP
- Les messages de demande et de réponse de masque d'adresse ICMP
- Le message de détection de routeur ICMP
- Le message de sollicitation de routeur ICMP
- Les messages de congestion et de contrôle de flux ICMP

- IP utilise le protocole ICMP pour signaler à l'émetteur des données qu'une erreur est survenue au cours du processus de livraison.
- Les messages ICMP sont transmis à l'aide du protocole IP ; leur livraison n'est donc pas fiable.
- Les messages de demande et de réponse d'écho ICMP permettent à l'administrateur réseau de tester la connectivité IP afin de faciliter le processus de dépannage.

Vue d'ensemble

Un routeur utilise un protocole de routage dynamique afin d'apprendre les routes menant aux réseaux de destination. Les routeurs utilisent généralement une combinaison de routage dynamique et de routes statiques entrées manuellement. Indépendamment de la méthode utilisée, lorsqu'un routeur identifie une route comme étant le meilleur chemin vers une destination, il l'installe dans sa table de routage. Ce module décrit les méthodes d'examen et d'interprétation du contenu de la table de routage.

Parmi tous les travaux réalisés par l'administrateur réseau, le dépannage et le test d'un réseau sont probablement les opérations les plus longues. Pour être efficace, un travail de test et de dépannage doit être effectué de manière logique et séquentielle, et sur la base d'une documentation précise. Sinon, les mêmes problèmes risquent de se reproduire et l'administrateur réseau ne parviendra jamais à réellement comprendre le réseau. Ce module décrit une approche structurée du dépannage d'un réseau et fournit les outils à utiliser lors du processus de dépannage.

Parmi tous les problèmes, les problèmes de routage sont très courants et très difficiles à diagnostiquer pour les administrateurs réseau. L'identification et la résolution des problèmes de routage peuvent ne pas paraître simples, mais de nombreux outils facilitent ce travail. Ce module présente les outils les plus importants et décrit leur utilisation.

À la fin de ce module, les étudiants doivent être en mesure de:

- Utiliser la commande **`show ip route`** pour recueillir des informations détaillées sur les routes installées sur le routeur
- Configurer une route ou un réseau par défaut
- Comprendre la manière dont un routeur utilise l'adressage des couches 2 et 3 pour déplacer des données sur le réseau
- Utiliser la commande **`ping`** pour effectuer des tests de connectivité réseau de base
- Utiliser la commande **`telnet`** pour vérifier le logiciel de la couche application entre des stations source et destinataire
- Effectuer un dépannage par test séquentiel des couches OSI
- Utiliser la commande **`show interfaces`** pour confirmer des problèmes au niveau des couches 1 et 2
- Utiliser les commandes **`show ip route`** et **`show ip protocol`** pour identifier des problèmes de routage
- Utiliser la commande **`show cdp`** pour vérifier la connectivité de la couche 2
- Utiliser la commande **`traceroute`** pour identifier le chemin emprunté par un paquet entre des réseaux
- Utiliser la commande **`show controllers serial`** pour vérifier le câblage
- Utiliser les commandes **`debug`** de base pour surveiller l'activité d'un routeur

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
9.1	Examen de la table de routage
9.2	Tests réseau
9.3	Vue d'ensemble du dépannage des problèmes de routeur

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
		• Utilisation du modèle OSI en tant que guide pour le dépannage systématique de réseau • Dépannage d'un équipement dans un réseau en fonctionnement • Exécution du dépannage d'un LAN simple • Dépannage de protocoles de routage • Dépannage de l'adressage IP et de la configuration des hôtes	

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
		• Utilisation du modèle OSI en tant que guide pour le dépannage systématique de réseau • Dépannage d'un équipement dans un réseau en fonctionnement • Exécution du dépannage d'un LAN et d'un VLAN • Dépannage de protocoles de routage • Dépannage de l'adressage IP et de la configuration des hôtes	

Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
• Utilisation d'un sous-ensemble de commandes Cisco IOS pour analyser et signaler les problèmes sur le réseau • Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	• Utilisation des commandes intégrées à l'IOS pour analyser et signaler les problèmes sur le Utilisation des protocoles intégrés de la couche 3 à la couche 7 pour établir, tester, interrompre ou arrêter la connectivité aux équipements distants à partir de la console du routeur	

9.1 Examen de la table de routage

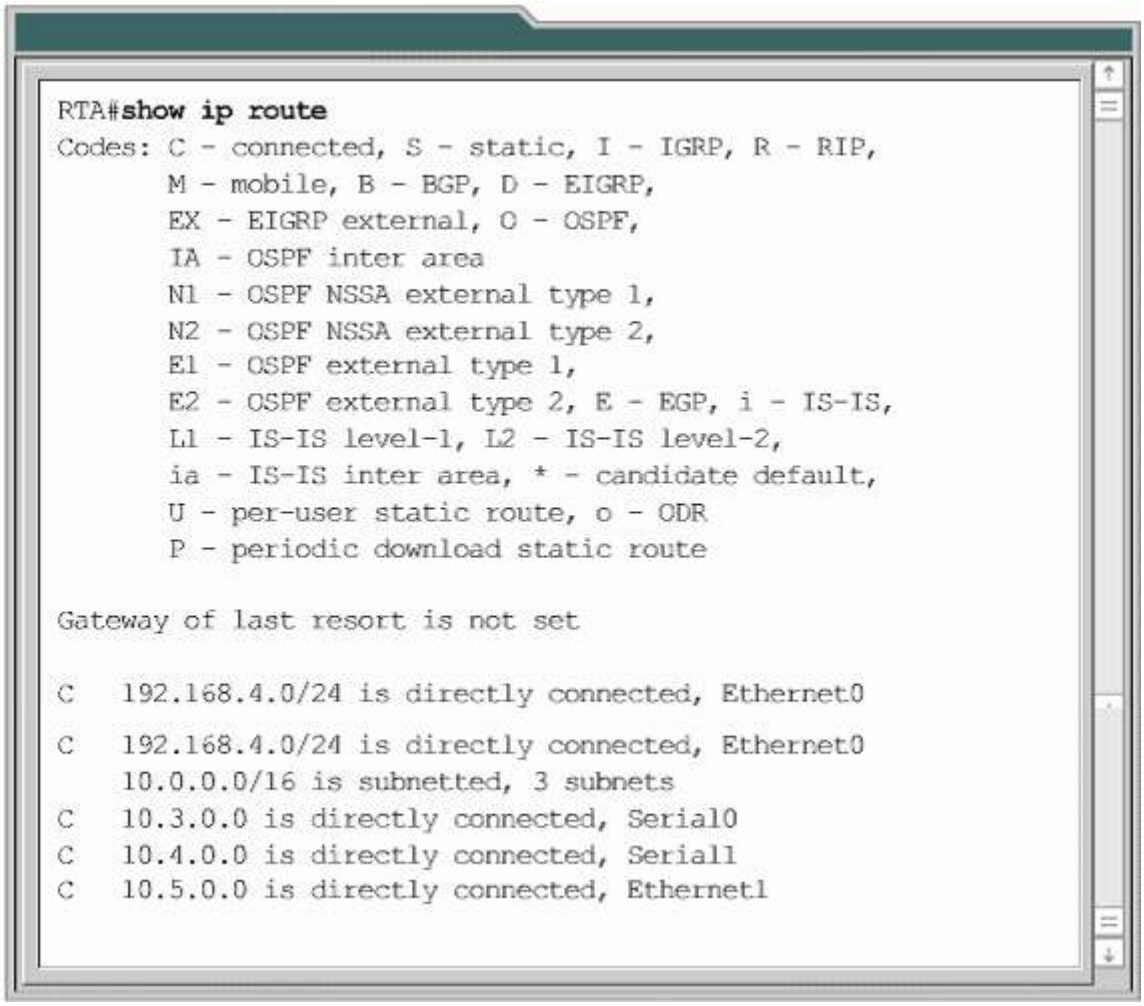
9.1.1 Commande show ip route

L'une des principales fonctions d'un routeur est de déterminer le meilleur chemin vers une destination donnée. Un routeur apprend les chemins, également appelés routes, à partir de la configuration d'un administrateur ou à partir d'autres routeurs par le biais de protocoles de routage. Les routeurs stockent cette information de routage dans des tables de routage à l'aide de la mémoire DRAM (Dynamic Random Access Memory) intégrée. Une table de routage contient la liste des meilleures routes disponibles. Les routeurs utilisent la table de routage pour prendre des décisions concernant la transmission des paquets.

La commande **`show ip route`** affiche le contenu de la table de routage IP. Cette table contient des entrées pour tous les réseaux et les sous-réseaux connus, ainsi qu'un code indiquant comment ces informations ont été apprises. Voici des exemples de commandes supplémentaires à utiliser avec la commande **`show ip route`**:

- **`show ip route connected`**
- **`show ip route`** *`address`*
- **`show ip route rip`**
- **`show ip route igrp`**
- **`show ip route static`**

Une table de routage associe des préfixes de réseau à une interface de sortie. 1



```
RTA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP,
       M - mobile, B - BGP, D - EIGRP,
       EX - EIGRP external, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2,
       E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EGP, i - IS-IS,
       L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, * - candidate default,
       U - per-user static route, o - ODR
       P - periodic download static route

Gateway of last resort is not set

C   192.168.4.0/24 is directly connected, Ethernet0
C   192.168.4.0/24 is directly connected, Ethernet0
    10.0.0.0/16 is subnetted, 3 subnets
C   10.3.0.0 is directly connected, Serial0
C   10.4.0.0 is directly connected, Serial1
C   10.5.0.0 is directly connected, Ethernet1
```

Lorsque RTA reçoit un paquet destiné à 192.168.4.46, il recherche le préfixe 192.168.4.0/24 dans sa table. RTA transmet ensuite le paquet via une interface (Ethernet0) sur la base de l'entrée de la table de routage. Si RTA reçoit un paquet destiné à 10.3.21.5, il l'envoie via une interface Serial 0.

Cet exemple de table de routage indique quatre routes pour des réseaux directement connectés. Ces routes, marquées d'un C, sont disponibles pour des réseaux directement connectés. RTA élimine tout paquet destiné à un réseau qui ne figure pas dans sa table de routage. Pour transmettre des paquets à d'autres destinations, il est nécessaire que la table de routage de RTA inclue davantage de routes. Ces nouvelles routes peuvent être ajoutées de l'une des manières suivantes:

- **Routage statique** – Un administrateur définit manuellement les routes vers un ou plusieurs réseaux de destination.
- **Routage dynamique** – Les routeurs suivent les règles définies par un protocole de routage pour échanger des informations de routage et sélectionner indépendamment le meilleur chemin.

Les routes définies par un administrateur sont dites «statiques», car elles ne changent pas tant que l'administrateur réseau ne programme pas manuellement des modifications. Les routes apprises des autres routeurs sont dites «dynamiques», car elles peuvent changer automatiquement lorsque les routeurs voisins se transmettent mutuellement des informations mises à jour. Chaque méthode présente des avantages et des inconvénients. 2 3

Avantages du routage statique	Inconvénients du routage statique
Faible surcharge du système. Les routeurs ne consacrent pas des cycles processeur entiers au calcul du meilleur chemin. La mémoire et la puissance de traitement nécessaires sont réduites (le routeur nécessaire est donc moins onéreux).	Haut niveau de maintenance de la configuration. Les administrateurs doivent configurer toutes les routes statiques manuellement. Les réseaux complexes peuvent nécessiter une reconfiguration constante.
Aucune utilisation de la bande passante. Les routeurs n'occupent pas la bande passante pour s'envoyer mutuellement des mises à jour à propos des routes statiques.	Absence d'adaptabilité. Les routes configurées statiquement ne peuvent pas être adaptées à des modifications d'état de lien.
Fonctionnement sécurisé. Le routage statique est plus sécuritaire car les routeurs n'envoient pas de mises à jour de routage. Par conséquent, aucune information réseau n'est transmise et ne peut être interceptée afin de planifier une attaque contre le réseau.	
Prévisibilité. Les routes statiques permettent à l'administrateur de contrôler précisément la sélection de chemin d'un routeur. Le routage dynamique conduit parfois à des résultats inattendus, même dans des réseaux de petite taille.	

Avantages du routage dynamique	Inconvénients du routage dynamique
Haut degré d'adaptabilité. Les routeurs peuvent s'alerter mutuellement à propos de liens hors service ou de chemins récemment découverts. Les routeurs "apprennent" automatiquement la topologie d'un réseau et sélectionnentles meilleurs chemins.	Surcharge système et utilisation élevée de la mémoire. Les processus de routage dynamique peuvent nécessiter une quantité significative de temps processeur et de mémoire
Faible niveau de maintenance de la configuration. Une fois que les paramètres de base d'un protocole de routage sont définis correctement, aucune intervention administrative n'est	Utilisation élevée de la bande passante. Les routeurs utilisent la bande passante pour envoyer et recevoir des mises à jour de routage, ce qui peut nuire aux performances

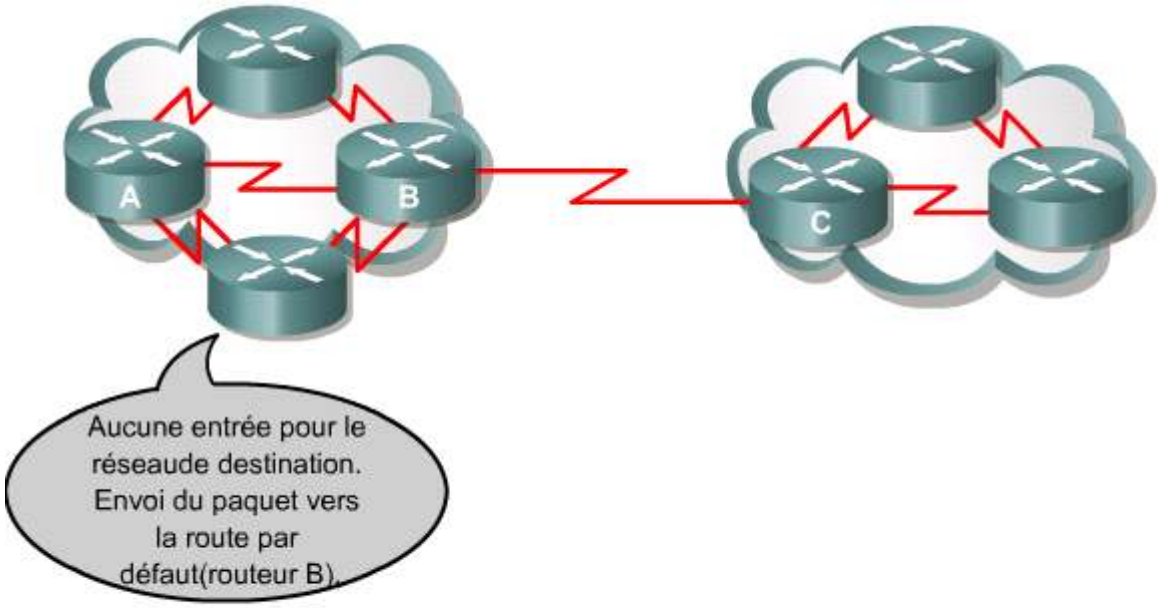
Activité de TP

Exercice : Utilisation de la commande **`show ip route`** pour examiner les tables de routage

Au cours de ce TP, les étudiants vont configurer un système d'adressage IP avec des réseaux de classe B

9.1 Examen de la table de routage
9.1.2 Détermination de la passerelle de dernier recours

Il n'est pas faisable, ni même souhaitable, pour un routeur de conserver des routes pour toutes les destinations possibles. À la place, les routeurs utilisent une route par défaut ou une passerelle de dernier recours. Les routes par défaut sont utilisées lorsque le routeur est incapable d'associer un réseau de destination à une entrée spécifique de la table de routage. Le routeur utilise cette route par défaut pour atteindre la passerelle de dernier recours lors d'une tentative de transmission d'un paquet. 1



Utilisation d'une route par défaut si le prochain saut ne figure pas explicitement dans la table de routage.

Le principal avantage au niveau de l'évolutivité est que, grâce aux routes par défaut, les tables de routage ne sont pas encombrées. Les routes par défaut permettent aux routeurs de transmettre des paquets destinés à n'importe quel hôte Internet sans avoir à mettre à jour une entrée de table pour chaque réseau Internet. Les routes par défaut peuvent être saisies par un administrateur de manière statique ou apprises de manière dynamique via un protocole de routage.

Le routage par défaut commence avec l'administrateur. Avant que des routeurs puissent échanger des informations de manière dynamique, un administrateur doit configurer au moins un routeur avec une route par défaut. Selon les résultats souhaités, un administrateur peut utiliser l'une des commandes suivantes pour configurer une route par défaut de manière statique: 2

Commande
Router(config)#**ip default-network** *[network number]*

La commande **ip default-network** définit une route par défaut candidate.

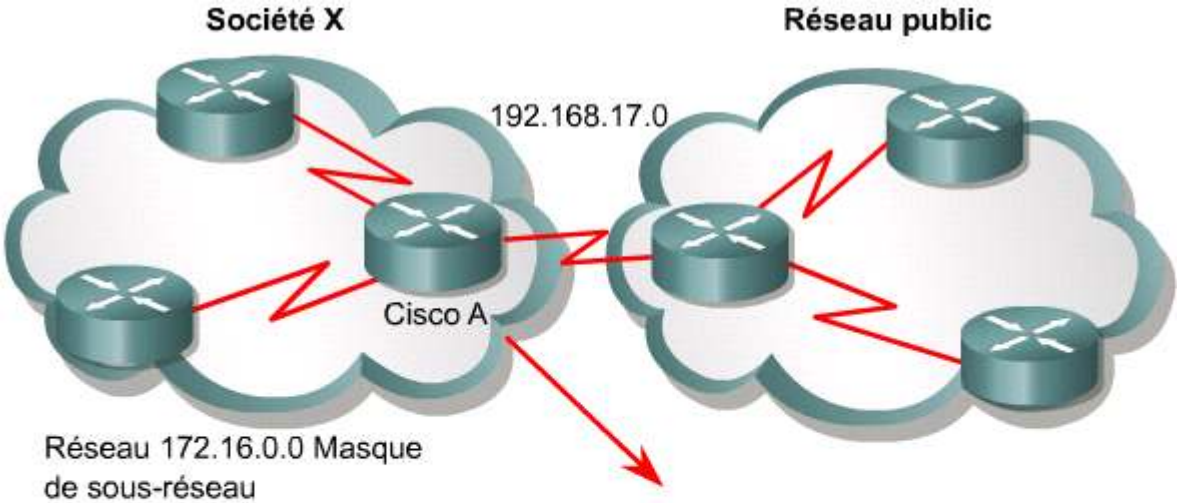
ip default-network
ou
ip route 0.0.0.0 0.0.0.0

La commande **ip default-network** est utilisée pour établir une route par défaut dans les réseaux où sont utilisés les protocoles de routage dynamique. La commande **ip default-network** s'utilise dans le système d'adressage avec classes (classful), ce qui signifie que si le routeur a une route vers un sous-réseau entré par cette commande, il n'installera en fait que la route vers le réseau principal non subneté.

La commande **`ip default-network`** doit être appliquée avec le réseau principal non subneté afin de positionner le drapeau candidate default route. 3

Commande ip default network	Description
`network-number`	Numéro du réseau ou du sous-réseau IP par défaut candidat.

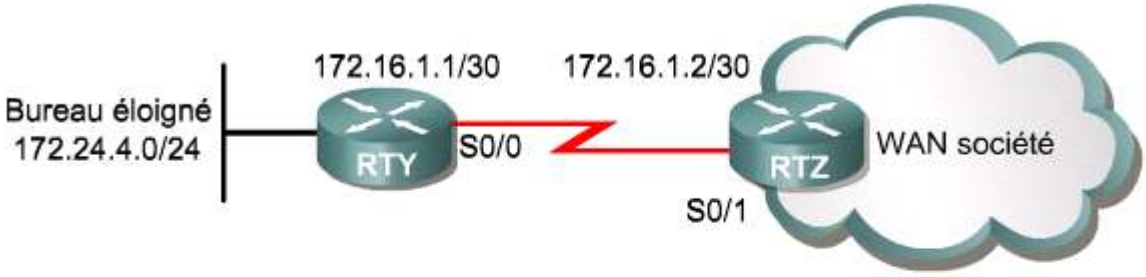
La commande globale **`ip default-network 192.168.17.0`** définit le réseau 192.168.17.0 de classe C comme chemin de destination pour les paquets qui ne comportent pas d'entrées dans la table de routage. Pour chaque réseau configuré avec **`ip default-network`**, si un routeur dispose d'une route correspondante, celle-ci est marquée comme route par défaut candidate. 4



Cisco A

```
Router(config)#router rip
Router(config-router)#network 172.16.0.0
Router(config-router)#network 192.168.17.0
Router(config-router)#exit
Router(config)#ip default-network 192.168.17.0
```

La création d'une **`ip route`** vers 0.0.0.0/0 est une autre manière de configurer une route par défaut. 5




```
RTY(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2
```

Si le réseau ne figure pas dans la table de routage du routeur RTY, ce dernier envoie le paquet à 172.16.1.2.

`Router(config)#ip route` `prefix mask {address | interface} [distance]`

Une fois que vous avez configuré une route par défaut ou un réseau par défaut, la commande **`show ip route`** affiche ce qui suit:

```
Gateway of last resort is 172.16.1.2 to network 0.0.0.0 6
```

Routeur

```
RTY#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP,
       M - mobile, B - BGP, D - EIGRP,
       EX - EIGRP external, O - OSPF,
       IA - OSPF inter area,
       N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2,
       E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EGP, i - IS-IS,
       L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, * - candidate default,
       U - per-user static route, o - ODR,
       P - periodic downloaded static route

Gateway of last resort is 172.16.1.2 to network 0.0.0.0

     172.16.0.0/30 is subnetted, 1 subnets

C    172.16.1.0 is directly connected, Serial0/0
     172.24.0.0/24 is subnetted, 1 subnets

C    172.24.4.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 172.16.1.2
```

Activité de TP

Exercice : Passerelle de dernier recours

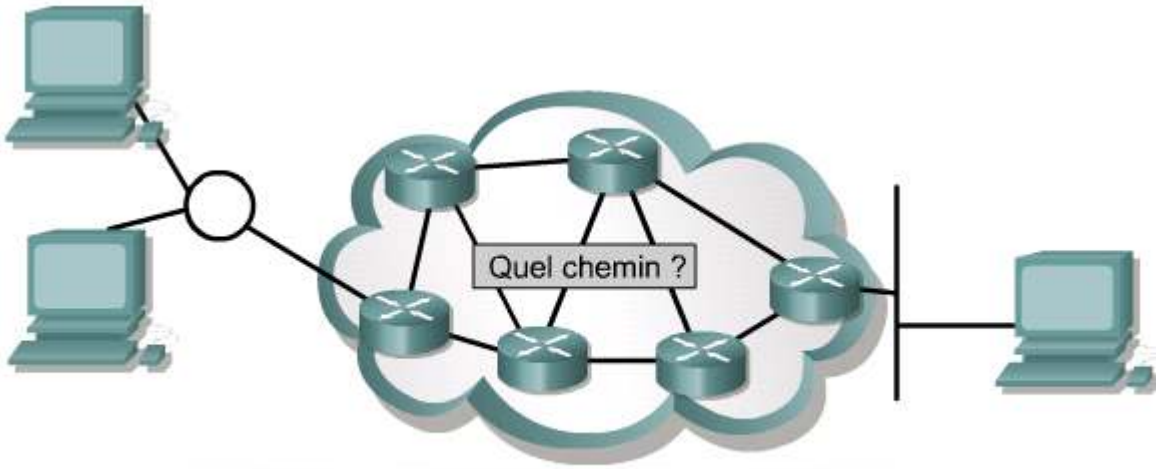
Au cours de ce TP, les étudiants vont configurer le protocole de routage RIP, ainsi que des routes par défaut (passerelles) sur les routeurs.

9.1 Examen de la table de routage

9.1.3 Détermination de la route entre la source et la destination

La détermination du chemin s'effectue au niveau de la couche réseau pour le trafic passant par un nuage. La fonction de détermination de chemin permet à un routeur d'évaluer les chemins disponibles vers une destination donnée et de définir le meilleur chemin pour traiter un paquet. Les services de routage utilisent les informations de topologie du réseau dans l'évaluation des chemins. Ces informations peuvent être configurées par l'administrateur réseau ou collectées par des processus dynamiques s'exécutant sur le réseau.

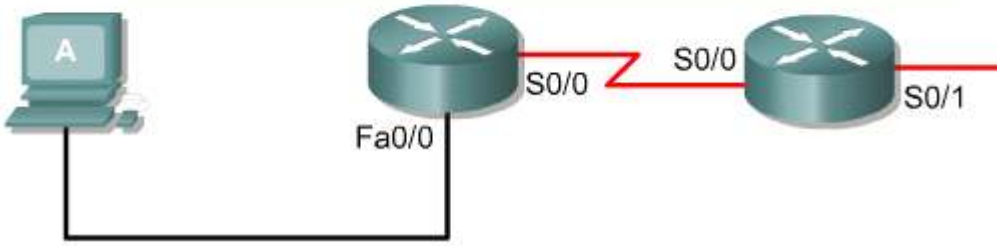
La couche réseau fournit un acheminement de bout en bout et au mieux des paquets à travers des réseaux interconnectés. Elle fait appel à une table de routage IP pour transmettre les paquets du réseau d'origine vers le réseau de destination. Une fois que le routeur a déterminé le chemin à utiliser, il prend le paquet sur une interface et le transmet à une autre interface ou à un port représentant le meilleur chemin vers la destination du paquet. 1 2



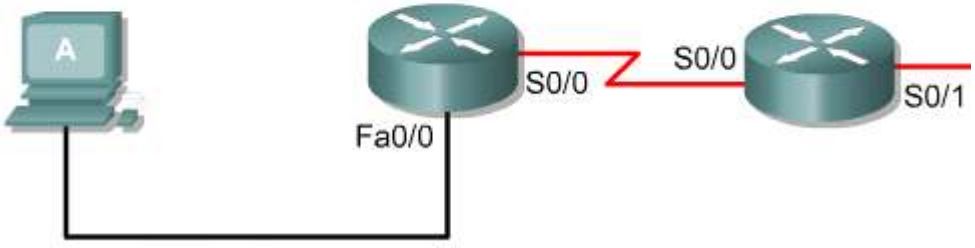
La couche 3 recherche le meilleur chemin dans l'interréseau.

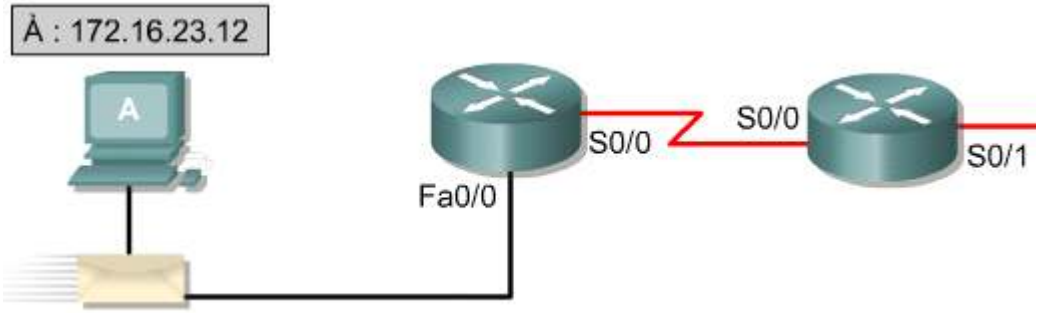
Fenêtre contextuelle

Une table de routage IP est constituée de paires " adresses réseau de destination et saut suivant ". Une entrée peut indiquer que pour atteindre le réseau 172.31.0.0, par exemple, le paquet doit être envoyé par l'interface S0/0. Le routage IP spécifie que les datagrammes IP se déplacent sur les interréseaux au rythme d'un saut à la fois. À chaque saut, la destination suivante est calculée en faisant correspondre l'adresse de destination du datagramme à une interface de sortie. S'il n'y a aucune correspondance, le datagramme est envoyé au routeur par défaut.

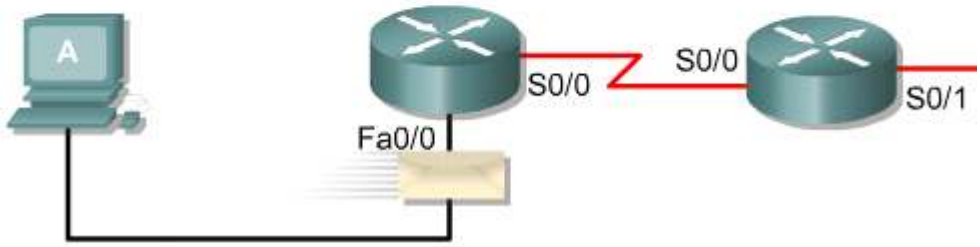


Réseau de destination	Interface (Saut suiv.)
172.16.0.0	S0/0
172.19.0.0	--
192.168.1.0	--
10.0.0.0	Fa0/0

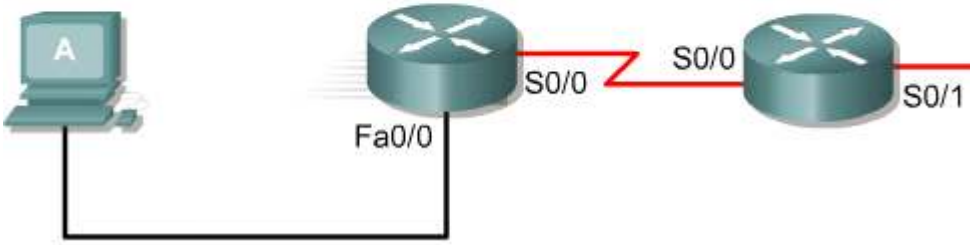




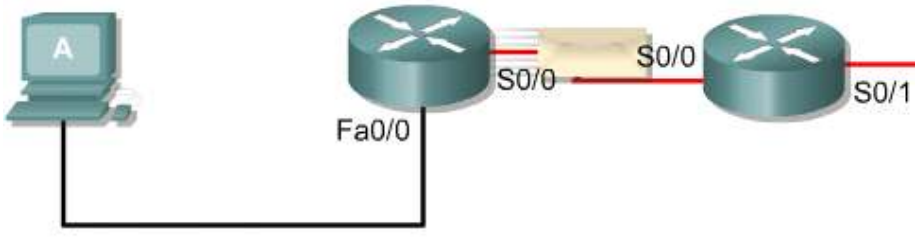
Réseau de destination	Interface (Saut suiv.)
172.19.0.0	--
192.168.1.0	--
10.0.0.0	Fa0/0



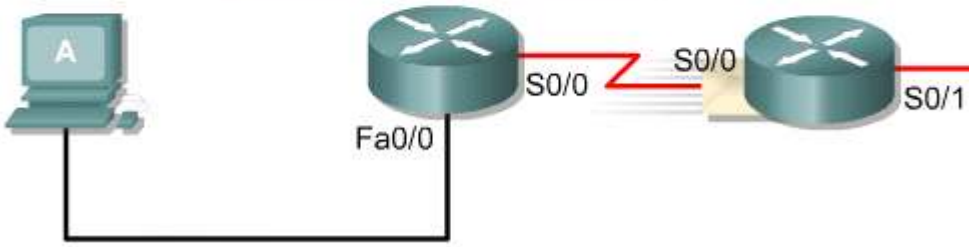
Réseau de destination	Interface (Saut suiv.)
172.16.0.0	S0/0
172.19.0.0	--
192.168.1.0	--
10.0.0.0	Fa0/0



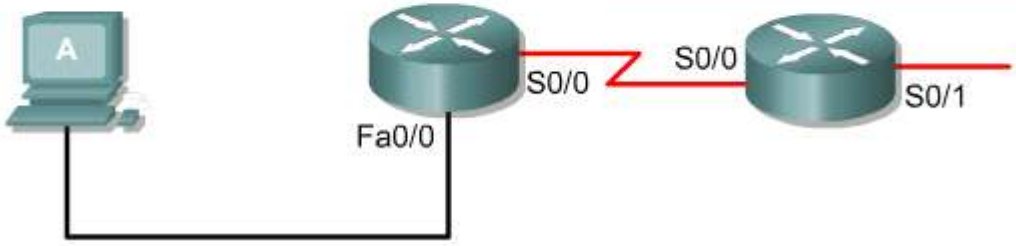
Réseau de destination	Interface (Saut suiv.)
172.16.0.0	S0/0
172.19.0.0	--
192.168.1.0	--
10.0.0.0	Fa0/0



Réseau de destination	Interface (Saut suiv.)
172.16.0.0	S0/0
172.19.0.0	--
192.168.1.0	--
10.0.0.0	Fa0/0

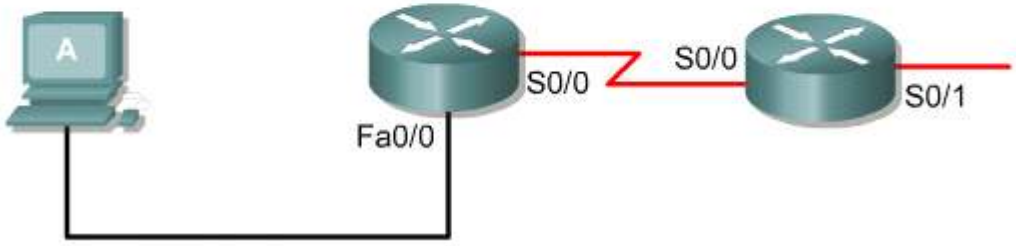


Réseau de destination	Interface (Saut suiv.)
172.16.0.0	S0/0
192.168.24.0	S0/1
Rout. par défaut	S0/1



Réseau de destination	Interface (Saut suiv.)
172.16.0.0	S0/0
192.168.24.0	S0/1
Rout. par défaut	S0/1

Pas de corresp.

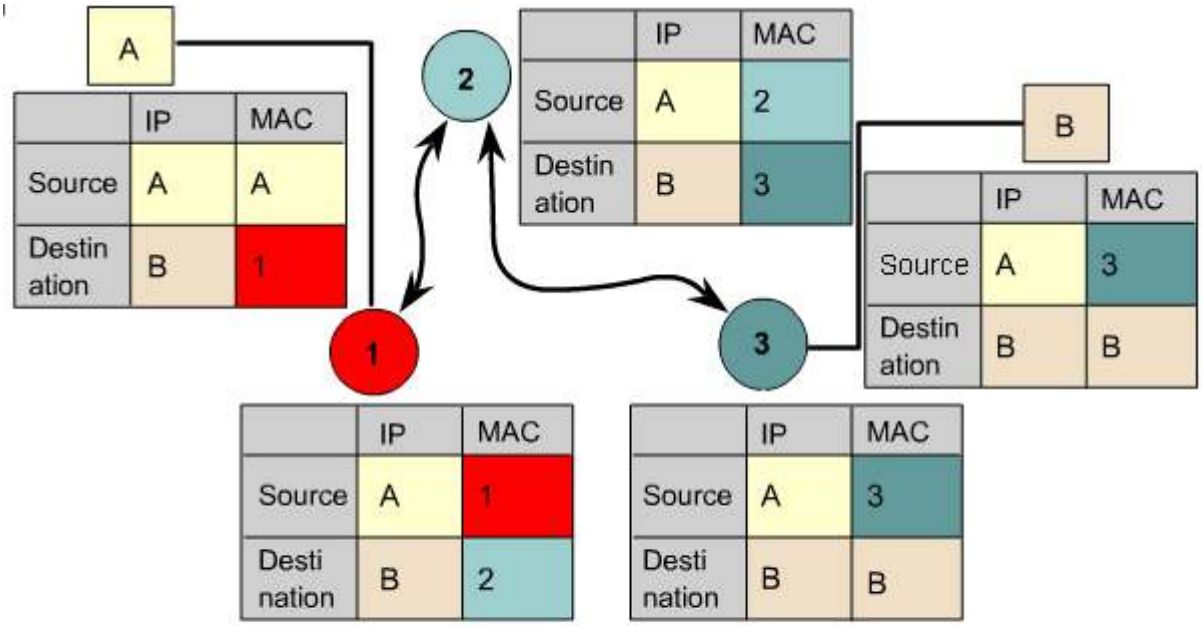


9.1 Examen de la table de routage

9.1.4 Détermination des adresses de couche 2 et 3

Alors que les adresses de couche réseau sont utilisées pour transmettre des paquets d'une source vers une destination, il est important de comprendre qu'un autre type d'adresse est utilisé pour transmettre les paquets d'un routeur vers le suivant. Pour acheminer un paquet de la source à la destination, des adresses de couche 2 et 3 sont utilisées. Comme l'illustre la figure 1, au niveau de chaque interface, tout au long du déplacement du paquet sur le réseau, la table de routage est examinée et le routeur détermine le saut suivant. Le paquet est ensuite transmis à l'aide de l'adresse MAC de ce saut suivant. Les adresses IP des unités source et destination ne changent à aucun moment.

L'adresse de couche 3 est utilisée pour acheminer le paquet du réseau source au réseau de destination. Les adresses IP d'origine et de destination restent identiques. L'adresse MAC change à chaque saut ou routeur. Une adresse de couche liaison de données est nécessaire, car l'acheminement au sein du réseau est déterminé par l'adresse figurant dans l'en-tête de trame de couche 2, et non dans l'en-tête de paquet de couche 3.



Au niveau de chaque interface, tout au long du déplacement du paquet sur le réseau, la table de routage est examinée et le routeur détermine le saut suivant. Le paquet est ensuite transmis à l'aide de l'adresse MAC du saut suivant. Les adresses IP des unités source et destination ne changent à aucun

Activité de média interactive

Glisser-Positionner : Adresse de couche 2 et 3

À la fin de cette activité, l'étudiant sera en mesure d'identifier les adresses de couche 2 et 3.

9.1 Examen de la table de routage

9.1.5 Détermination de la distance administrative de la route

Un routeur peut découvrir des routes à l'aide de protocoles de routage dynamiques ou un administrateur peut configurer manuellement des routes sur le routeur. Une fois que les routes ont été découvertes ou configurées, le routeur doit sélectionner les meilleures routes vers les réseaux.

La distance administrative de la route est l'information clé que le routeur utilise pour décider du meilleur chemin vers une destination en particulier. La distance administrative est un nombre qui mesure la fiabilité de la source des informations de route. Plus la distance administrative est petite, plus la source est fiable.

Des protocoles de routage différents ont des distances administratives par défaut différentes. 1 Si un chemin a la distance administrative la plus petite, il est installé dans la table de routage. Une route n'est pas installée dans la table de routage si la distance administrative à partir d'une autre source est plus petite.

Protocoles	Distances administratives par défaut
Connected	0
Static	1
Route sommaire EIGRP	5
eBGP	20
EIGRP (interne)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP (externe)	170
iBGP (externe)	200

Activité de TP

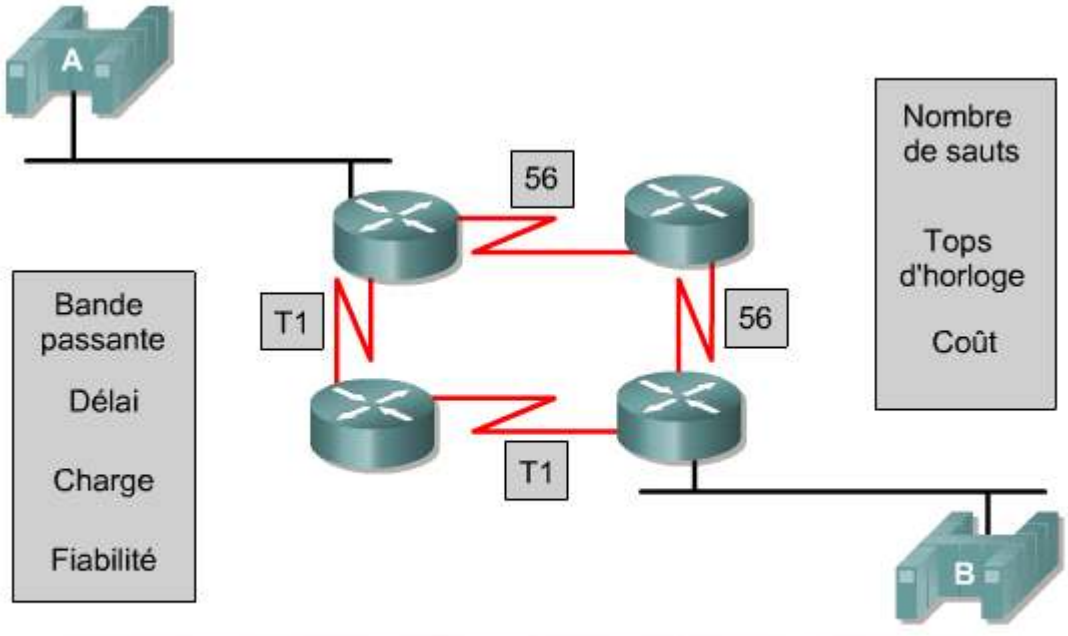
Activité en ligne : Distance administrative

Au cours de ce TP, les étudiants vont analyser les conséquences de l'utilisation de deux protocoles de routage.

9.1 Examen de la table de routage

9.1.6 Détermination de la métrique de la route

Les protocoles de routage utilisent des métriques pour déterminer la meilleure route vers une destination. La métrique est une valeur qui mesure les avantages d'une route. Certains protocoles de routage utilisent un seul facteur pour calculer une métrique. Par exemple, le protocole RIP version 1 (RIP v1) utilise le nombre de sauts comme unique facteur de détermination de la métrique d'une route. D'autres protocoles basent leur métrique sur le nombre de sauts, la bande passante, le délai, la charge, la fiabilité, le délai de tops d'horloge et le coût. [1]

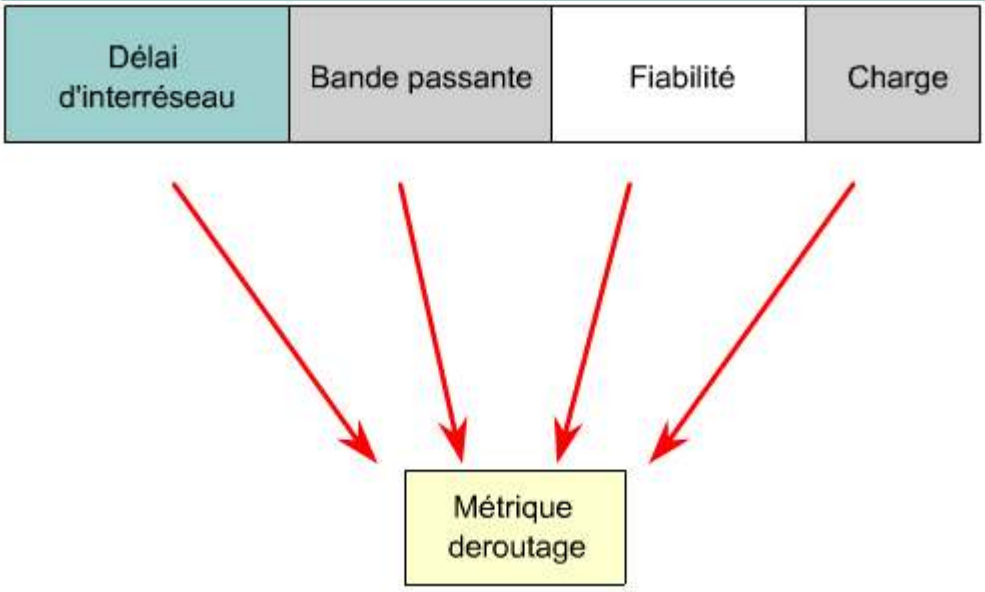


Est-ce qu'une route alternative peut servir de substitut à une route non disponible ?

Chaque algorithme de routage interprète à sa façon les meilleures informations. L'algorithme génère un nombre, appelé valeur métrique, pour chaque chemin du réseau. Normalement, plus ce nombre est petit, meilleur est le chemin.

Des facteurs, tels que la bande passante et le délai, sont statiques, car ils restent identiques pour chaque interface jusqu'à ce que le routeur soit reconfiguré ou que le réseau soit restructuré. Des facteurs, tels que la charge et la fiabilité, sont dynamiques, car ils sont calculés en temps réel par le routeur pour chaque interface. [2] [3]

Métrique	Description
Nombre de sauts	Nombre de routeurs à traverser pour atteindre une destination. Le chemin comportant le plus petit nombre de sauts est privilégié.
Bande passante	Vitesse de la liaison. Le chemin comportant la plus grande bande passante est privilégié.
Délai	Durée de déplacement d'un paquet sur une liaison. Le chemin dont le délai est le plus court est privilégié.
Charge	Volume d'activité sur une liaison. Sur les routeurs Cisco, cette valeur est généralement comprise entre 1 et 255, où 1 représente la liaison dont la charge est la plus faible et 255, la liaison dont la charge est la plus élevée. Les chemins dont la charge est la plus faible sont privilégiés.
Fiabilité	Degré d'erreur sur une liaison. Sur les routeurs Cisco, cette valeur est généralement comprise entre 1 et 255, où 255 représente la liaison dont le degré de fiabilité est le plus élevé. Les chemins à haut degré de fiabilité sont privilégiés.
Coût	Métrique définie par l'administrateur. Les chemins à moindre coût sont privilégiés.



Plus le nombre de facteurs utilisés pour créer une métrique est élevé, plus la souplesse de personnalisation du réseau en fonction de besoins spécifiques est grande. Par défaut, le protocole IGRP utilise deux facteurs statiques (bande passante et délai) pour calculer une valeur métrique. Ces deux facteurs peuvent être configurés manuellement, ce qui permet un contrôle précis sur les routes qu'un routeur choisit. IGRP peut également être configuré pour inclure des facteurs dynamiques (charge et fiabilité) dans le calcul de la métrique. En utilisant des facteurs dynamiques, les routeurs IGRP peuvent prendre des décisions sur la base des conditions actuelles. Si une liaison devient particulièrement chargée ou non fiable, IGRP augmente la métrique des routes qui utilisent cette liaison. D'autres routes peuvent présenter une valeur métrique plus petite que la route dont la métrique a été abaissée et donc être utilisées à sa place.

IGRP calcule la métrique en ajoutant les valeurs pondérées des différentes caractéristiques de la liaison au réseau en question. Dans l'exemple suivant, les valeurs de bande passante, de bande passante divisée par la charge et de délai sont pondérées avec les constantes K1, K2 et K3.

Métrique = [K1 * bande passante + (K2 * bande passante)/(256-charge) + K3*délai] * [K5/(fiabilité + K4)]

Les valeurs par défaut des constantes sont K1 = K3 = 1 et K2 = K4 = K5 = 0.

Si K5 = 0, le terme [K5/(fiabilité + K4)] n'est pas utilisé. Selon les valeurs par défaut des constantes K1 à K5, le calcul de la métrique composite utilisé par IGRP se réduit alors à l'expression suivante:

Métrique = bande passante + délai.

Activité de média interactive

Glisser-Positionner : Métrique de route

À la fin de cette activité, l'étudiant sera en mesure de comprendre la métrique d'une route.

9.1 Examen de la table de routage

9.1.7 Détermination du saut suivant de la route

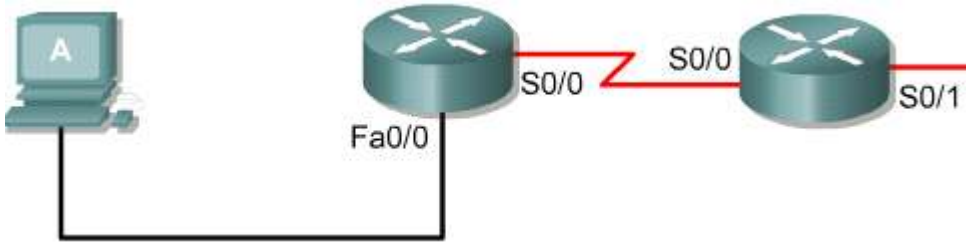
Les algorithmes de routage insèrent diverses informations dans les tables de routage. Les associations destination/saut suivant indiquent à un routeur qu'une destination donnée peut être atteinte de manière optimale par l'envoi du paquet à un routeur en particulier. Ce routeur représente le saut suivant sur le chemin vers la destination finale. 1

Fenêtre contextuelle

Les sauts suivants sont indiqués en rouge dans cet exemple d'informations affichées par la commande show ip route.

```
rtl#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP,
       M - mobile, B - BGP, D - EIGRP,
       EX - EIGRP external, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EGP i - IS-IS,
       L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, * - candidate default,
       U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R   200.200.200.0/24 [120/1] via 192.168.10.2, 00:00:14,
Serial0/0

C   192.168.10.0/24 is directly connected, Serial0/0
C   192.168.0.0/24 is directly connected, Loopback0
rtl#show ip route 200.200.200.0
Routing entry for 200.200.200.0/24
 Known via "rip", distance 120, metric 1
 Redistributing via rip
 Last update from 192.168.10.2 on Serial0/0, 00:00:11
ago
 Routing Descriptor Blocks:
 * 192.168.10.2, from 192.168.10.2, 00:00:11 ago, via
Serial0/0
   Route metric is 1, traffic share count is 1
```

Lorsqu'un routeur reçoit un paquet entrant, il vérifie l'adresse de destination et tente de faire correspondre cette adresse avec le saut suivant. 2



Utilisez les commandes suivantes pour rechercher la dernière mise à jour de routage:

- **show ip route** 1

```
rtl#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP,
       M - mobile, B - BGP, D - EIGRP,
       EX - EIGRP external, O - OSPF,
       IA - OSPF inter area,
       N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2,
       E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EGP, i - IS-IS,
       L1 - IS-IS level-1, L2 - IS-IS level-2,
       ia - IS-IS inter area, * - candidate default,
       U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R  200.200.200.0/24 [120/1] via 192.168.10.2, 00:00:14,
Serial0/0
C  192.168.10.0/24 is directly connected, Serial0/0
C  192.168.0.0/24 is directly connected, Loopback0
rtl#show ip route 200.200.200.0
Routing entry for 200.200.200.0/24
 Known via "rip", distance 120, metric 1
 Redistributing via rip
 Last update from 192.168.10.2 on Serial0/0, 00:00:11
ago
 Routing Descriptor Blocks:
 * 192.168.10.2, from 192.168.10.2, 00:00:11 ago, via
Serial0/0
   Route metric is 1, traffic share count is 1
```

- **show ip route** *address* 1
- **show ip protocols** 2

```
rt1#show ip protocols
Routing Protocol is "rip"
 Sending updates every 30 seconds, next due in 9
seconds
 Invalid after 180 seconds, hold down 180, flushed
after 240
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Redistributing: rip
 Default version control: send version 1, receive
any version
   Interface    Send Recv Triggered RIP Key-chain
   Serial0/0    1  1 2
   Loopback0    1  1 2
 Routing for Networks:
   192.168.0.0
   192.168.10.0
 Routing Information Sources:
   Gateway    Distance    Last Update
   192.168.10.2    120    00:00:03
 Distance: (default is 120)
```

- **show ip rip database** 3

```
rt1#show ip rip database
192.168.0.0/24    auto-summary
192.168.0.0/24    directly connected, Loopback0
192.168.10.0/24    auto-summary
192.168.10.0/24    directly connected, Serial0/0
200.200.200.0/24    auto-summary
200.200.200.0/24
[1] via 192.168.10.2, 00:00:20, Serial0/0
```

Fenêtre contextuelle

La partie en rouge (00:00:20) indique que la dernière mise à jour RIP est survenue il y a vingt secondes.

Activité de TP

Exercice : Dernière mise à jour des routesAu cours de ce TP, l'étudiant va collecter des informations sur les mises à jour de routage et sur les protocoles de routage.

9.1 Examen de la table de routage

9.1.9 Observation de chemins multiples vers une destination

Certains protocoles de routage prennent en charge plusieurs chemins vers la même destination. Contrairement aux algorithmes de chemin unique, ces algorithmes multi-chemins permettent un trafic sur plusieurs lignes, fournissent un meilleur débit et sont plus fiables.

IGRP supporte l'équilibrage de charge de coût différent qui est mieux connu sous le nom de variance. La commande **variance** demande au routeur d'inclure aussi les routes avec une métrique inférieure à n fois la métrique minimum pour la meilleure route pour cette destination, où n est le nombre spécifié par la commande de variance. La variable n peut prendre une valeur entre 1 et 128, avec comme valeur par défaut 1, ce qui signifie un partage de charge de coût égal.

Rt1 a deux routes pour le réseau 192.168.30.0. La commande variance va être placée sur Rt1 pour s'assurer que les deux chemins vers le réseau 192.168.30.0 sont utilisés.

```
rt1#show ip route
----Affichage tronqué----
Gateway of last resort is not set
I  192.168.30.0/24 [100/8986] via 192.168.0.2, 00:00:35, FastEthernet0/0
----Affichage tronqué----
```

La figure 1 montre les informations affichées par **show ip route** sur Rt1 avant la configuration de variance. L'interface Fast Ethernet 0/0 est la seule route pour le réseau 192.168.30.0. Cette route a une distance administrative de 100 et une métrique de 8986.

```
rt1#show ip route
----output omitted----
Gateway of last resort is not set
I  192.168.30.0/24 [100/8986] via 192.168.0.2,
 00:00:22, FastEthernet0/0 [100/10976] via
 192.168.10.2, 00:00:22, Serial0/0

----output omitted----
```

La figure 2 montre les informations affichées par **show ip route** sur Rt1 après la configuration de variance. La route préférée est l'interface Fast Ethernet 0/0, mais l'interface Serial 0/0 peut aussi être utilisée. Après que la commande variance ait été exécutée, IGRP va faire du partage de charge entre les deux liens.

La route privilégiée est l'interface FastEthernet 0/0, mais l'interface Serial 0/0 peut également être utilisée. Pour vérifier l'équilibrage de charge, envoyez une requête **ping** au réseau 192.168.30.1.

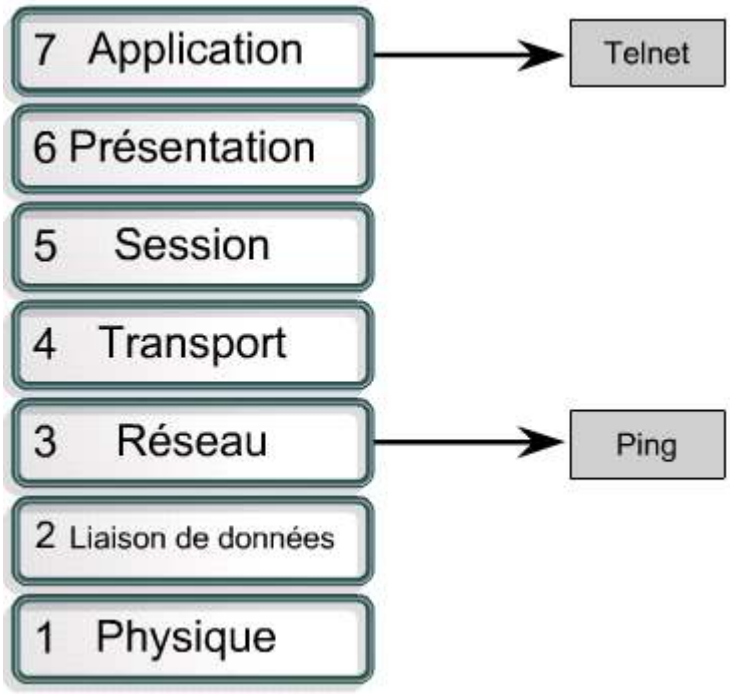
Une fois la commande **ping** exécutée, la route privilégiée passe par l'interface Serial 0/0. Le protocole IGRP utilise l'équilibrage de charge entre les deux liaisons. 3

```
rt1#show ip route
----output omitted----
Gateway of last resort is not set
I  192.168.30.0/24 [100/8986] via 192.168.0.2,
 00:00:22, FastEthernet0/0 [100/10976] via
 192.168.10.2, 00:00:22, Serial0/0

----output omitted----
```

9.2 Tests réseau

9.2.1 Introduction aux tests réseau

Les tests de base d'un réseau doivent être effectués séquentiellement, selon l'ordre des couches du modèle de référence OSI. [1] Il est préférable de commencer par la couche 1, jusqu'à la couche 7 si nécessaire. Au niveau de la couche 1, cherchez à identifier des problèmes simples, tels que des cordons d'alimentation déconnectés d'une prise murale. Les problèmes les plus fréquents sur les réseaux IP proviennent d'erreurs dans le système d'adressage. Il est important de vérifier la configuration des adresses avant de passer aux autres étapes de configuration.

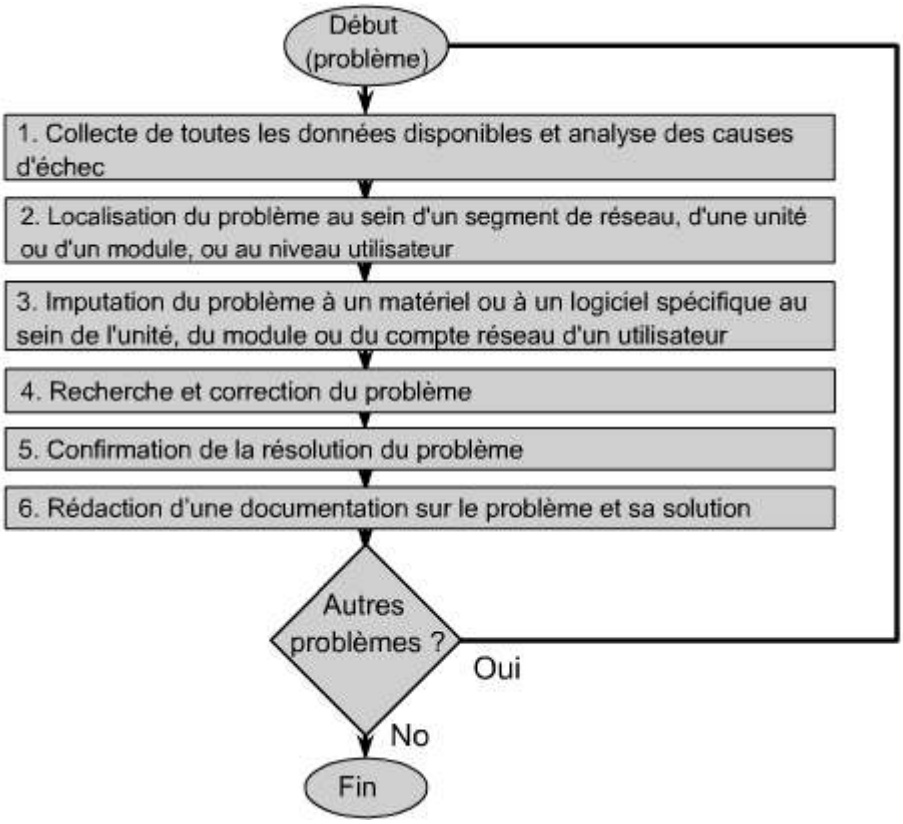


Chaque test décrit dans cette section est axé sur le fonctionnement d'un réseau au niveau d'une couche donnée du modèle OSI. Les commandes **`telnet`** et **`ping`** sont deux commandes importantes utilisées pour tester un réseau.

9.2 Tests réseau

9.2.2 Utilisation d'une approche structurée du dépannage

Le dépannage est un processus qui permet à un utilisateur de localiser les problèmes sur un réseau. Ce processus de dépannage devrait être basé sur des normes de gestion de réseau mises en place par un administrateur réseau. La création d'une documentation est très importante pour le processus de dépannage. [1]



Les étapes de ce modèle sont les suivantes:

Étape 1: Collecte de toutes les données disponibles et analyse des causes d'échec

Étape 2: Localisation du problème au sein d'un segment de réseau, d'une unité ou d'un module, ou au niveau utilisateur

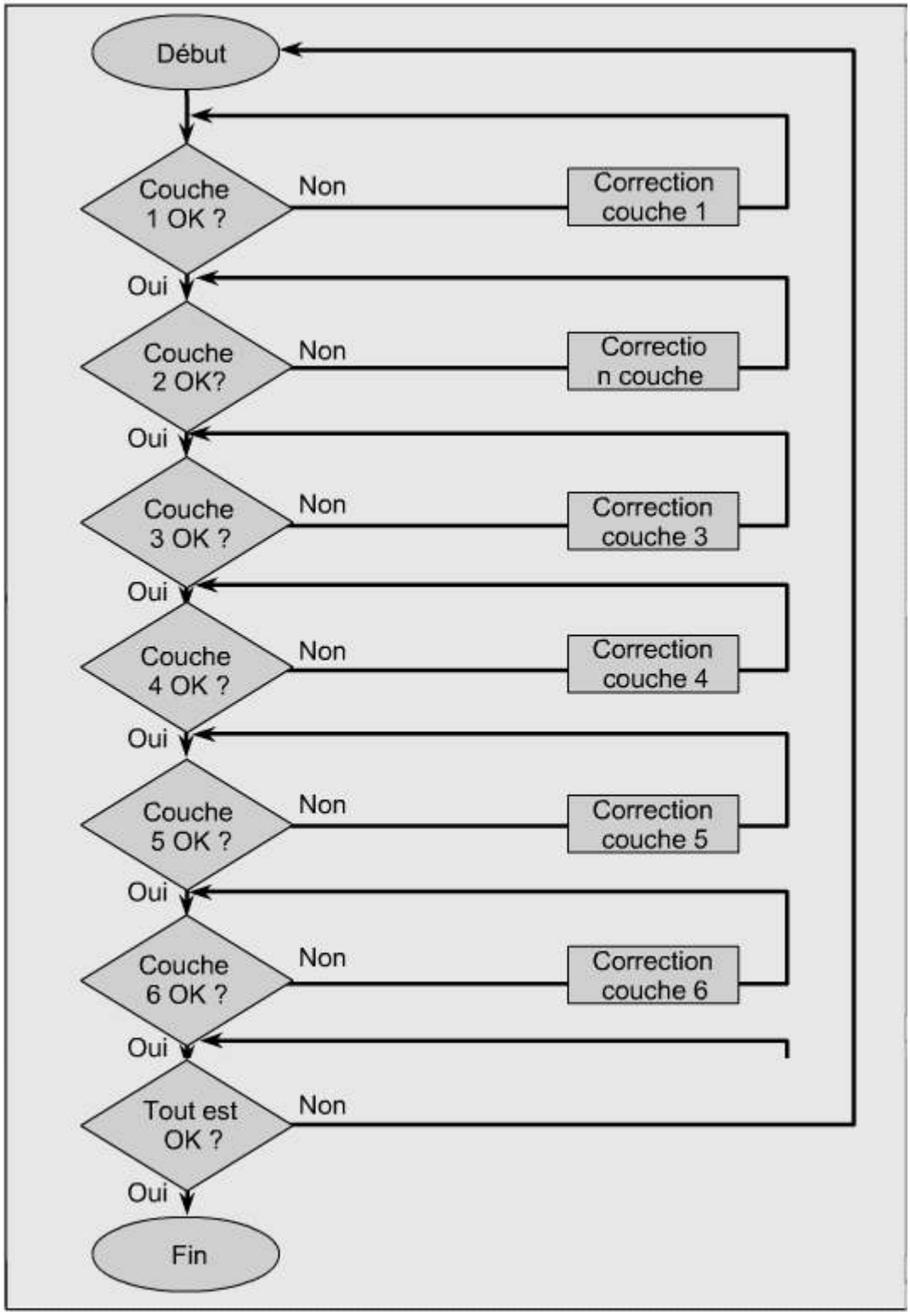
Étape 3: Imputation du problème à un matériel ou à un logiciel spécifique au sein de l'unité, du module ou du compte réseau d'un utilisateur

Étape 4: Recherche et correction du problème

Étape 5: Confirmation de la résolution du problème

Étape 6: Rédaction d'une documentation sur le problème et sa solution

La figure 2 illustre une autre approche du dépannage. Le dépannage ne se limite pas à ces deux méthodes. Toutefois, le recours à un processus structuré est d'une importance capitale pour le fonctionnement efficace et sans coupure d'un réseau.



Par le biais d'une approche structurée du dépannage, chaque membre d'une équipe de support de réseau peut connaître les opérations que chacun a réalisées pour résoudre un problème. Si diverses solutions de dépannage sont testées sans aucune organisation ni documentation, la résolution des problèmes n'est pas efficace. Même si un problème est résolu dans le cadre d'une approche non structurée, il sera probablement impossible de reproduire la solution lorsque des problèmes similaires surviendront ultérieurement.

Activité de média interactive

Glisser-Positionner : Dépannage

À la fin de cette activité, l'étudiant sera en mesure de comprendre la commande show interface.

9.2 Tests réseau

9.2.3 Test sur la base des couches OSI

La phase de test doit commencer au niveau de la couche 1 du modèle OSI, jusqu'à la couche 7 si nécessaire.

Les erreurs identifiées au niveau de la couche 1 peuvent être les suivantes: 1

- Câbles rompus
- Câbles déconnectés
- Câbles raccordés à des ports inappropriés
- Connexions instables
- Câbles inappropriés pour la tâche à accomplir (les câbles console, les câbles croisés et les câbles droits doivent être employés à bon escient)
- Problèmes d'émetteur-récepteur
- Problèmes de câblage ETCD
- Problèmes de câblage ETTD
- Unités hors tension

Les erreurs identifiées au niveau de la couche 2 peuvent être les suivantes: 2

- Interfaces série configurées de façon incorrecte
- Interfaces Ethernet configurées de façon incorrecte
- Ensemble d'encapsulation inapproprié (HDLC est utilisé par défaut pour les interfaces série)
- Fréquence d'horloge inappropriée pour les interfaces série
- Problèmes de carte réseau (NIC)

Les erreurs identifiées au niveau de la couche 3 peuvent être les suivantes:

- Protocole de routage non activé
- Protocole de routage incorrect activé
- Adresses IP incorrectes
- Masques de sous-réseau incorrects

Si des erreurs apparaissent sur le réseau, le processus de test basé sur les couches OSI doit être déclenché. La commande **`ping`** est utilisée pour tester la connectivité au niveau de la couche 3. La commande **`telnet`** peut être utilisée au niveau de la couche 7 pour vérifier le logiciel de la couche application entre des stations source et de destination. Ces deux commandes sont décrites plus loin dans une autre section de ce document.

Activité de média interactive

Associer : Tests avec les couches OSI

À la fin de cette activité, l'étudiant sera en mesure de comprendre les couches OSI.

9.2 Tests réseau

9.2.4 Dépannage de la couche 1 à l'aide des témoins lumineux

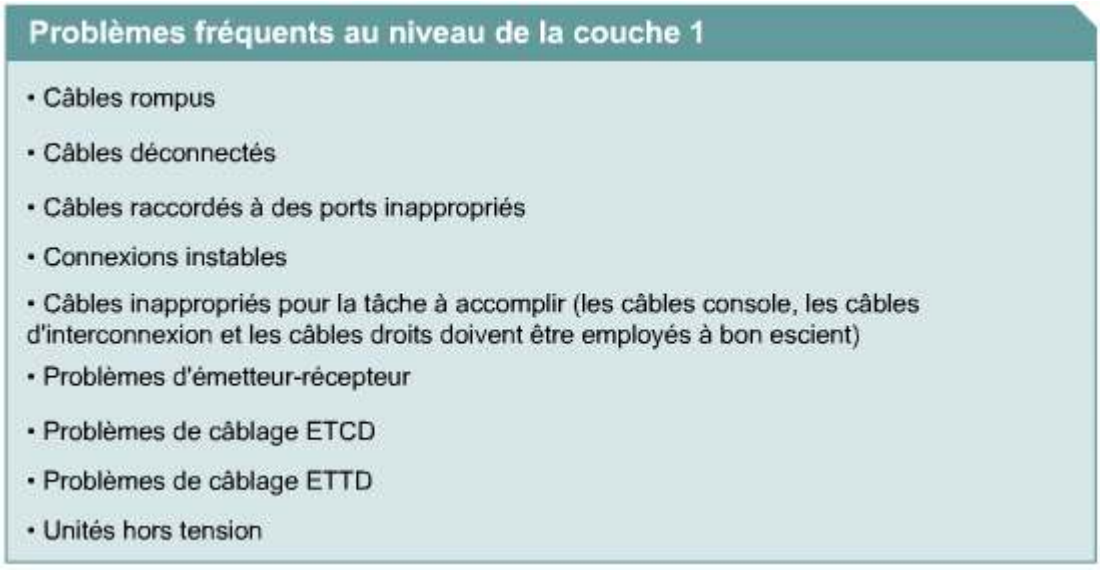
Les témoins lumineux sont utiles au dépannage. La plupart des interfaces ou des cartes réseau comportent des témoins lumineux qui indiquent si la connexion est valide. Ces témoins lumineux sont souvent appelés voyants de liaison. L'interface peut également disposer de témoins lumineux pour indiquer si le trafic est en cours de transmission (TX) ou reçu (RX). Si l'interface comporte des témoins lumineux indiquant que la connexion n'est pas valide, mettez l'unité hors tension et replacez la carte d'interface. Un voyant de liaison peut également indiquer une mauvaise connexion ou l'absence de liaison à cause d'un câble inapproprié ou défectueux.

Vérifiez que tous les câbles sont connectés aux ports appropriés. Vérifiez que toutes les interconnexions sont raccordées au bon emplacement à l'aide du câble et de la méthode appropriés. Vérifiez que tous les ports de concentrateur et de commutateur sont associés au réseau VLAN ou au domaine de collision approprié, et que les options de Spanning Tree correspondantes, entre autres, sont définies correctement.

Vérifiez que le câble approprié est utilisé. Un câble croisé peut être requis pour des connexions directes entre deux commutateurs ou concentrateurs, ou entre deux hôtes, tels que des PC ou des routeurs. Vérifiez que le câble de l'interface source est correctement connecté et en bon état. En cas de doute sur la connexion, replacez le câble et vérifiez la sécurité de la connexion. Essayez de remplacer le câble par un câble de travail connu. Si ce câble est connecté à une prise murale, utilisez un testeur de câble pour vérifier que la prise est correctement raccordée.

Vérifiez également le type, la connexion et la configuration de tout émetteur-récepteur utilisé. Si le remplacement du câble ne résout pas le problème, essayez de remplacer l'émetteur-récepteur si vous en utilisez un.

Assurez-vous également que l'unité est bien sous tension. Contrôlez toujours les composants de base avant d'exécuter des diagnostics ou de tenter un dépannage plus complexe. [1]



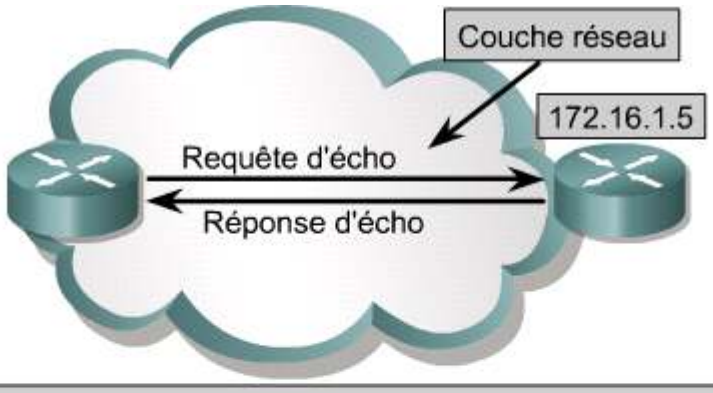
9.2 Tests réseau

9.2.5 Dépannage de la couche 3 à l'aide de la commande ping

L'utilitaire **ping** permet de tester la connectivité du réseau. Un grand nombre de protocoles réseau prennent en charge un protocole d'écho qui contribue à faciliter le diagnostic de la connectivité de base d'un réseau. Les protocoles d'écho permettent de vérifier si les paquets de protocole sont acheminés. La commande **ping** envoie un paquet à l'hôte de destination et attend un paquet de réponse de celui-ci. Les résultats du protocole d'écho peuvent aider à évaluer la fiabilité chemin-hôte et les délais sur le chemin. Ils permettent aussi de déterminer si l'accès à l'hôte est possible et si ce dernier fonctionne. Les informations affichées par la requête **ping** indiquent les temps minimum, moyen et maximum que prend un paquet de requêtes ping pour trouver un système donné et revenir. La commande **ping** utilise le protocole ICMP (Internet Control Message Protocol) pour vérifier la connexion matérielle et l'adresse logique au niveau de la couche réseau. Le tableau de la figure 1 indique les différents types de message ICMP. Il s'agit d'un mécanisme de test des plus élémentaires pour la connectivité du réseau.

Message	Usage
Destination inaccessible	Indique à l'hôte source qu'un paquet ne peut pas être livré.
Dépassement du délai	Le délai de livraison d'un paquet a expiré ; le paquet a été éliminé.
Épuisement de la source	La source envoie les données plus rapidement qu'elles ne peuvent être transmises. Ce message invite l'émetteur à ralentir.
Redirection	Le routeur qui envoie ce message a reçu un paquet pour lequel une autre route aurait pu être privilégiée. Ce message invite l'émetteur à utiliser la route la plus optimale.
Écho	Ce message est utilisé par la commande ping pour vérifier la connectivité.
Problème de paramètre	Ce message est utilisé pour identifier un paramètre qui est incorrect.
Horodatage	Ce message est utilisé pour mesurer le délai entre deux hôtes.
Demande de masque d'adresse/réponse à la demande	Ce message est utilisé pour demander et connaître le masque de sous-réseau à utiliser.
Annonce et sélection de routeur	Ce message permet aux hôtes de connaître de manière dynamique les adresses IP des routeurs connectés au sous-réseau.

Dans la figure 2, la cible 172.16.1.5 de la commande **ping** a répondu correctement aux cinq datagrammes envoyés. Les points d'exclamation (**!**) indiquent chaque écho réussi. Si votre écran affiche un ou plusieurs points (.) au lieu de points d'exclamation, cela signifie que le délai d'attente de l'application du routeur a expiré (ou encore, a été dépassé) pendant qu'elle attendait un écho de paquet de la cible précisée dans la commande **ping**.




```
Router>ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>
```

La commande suivante active un outil de diagnostic qui est utilisé pour vérifier la connectivité:

```
Router#ping [protocole] {hôte | adresse}
```

La commande **ping** teste les connexions du réseau en envoyant des requêtes d'écho ICMP à un hôte cible et en écoutant les réponses. La commande **ping** vérifie le nombre de paquets envoyés, le nombre de réponses reçues et le pourcentage de paquets perdus. Elle vérifie également le temps nécessaire pour que les paquets atteignent leur destination et pour que les réponses soient reçues. Ces informations permettent de contrôler la communication entre une station de travail et d'autres hôtes, et si des données ont été perdues. 2

Router

```
R1#ping
Protocol [ip]:
Target IP address: 172.16.1.5
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 172.16.2.33
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 36/36/36 ms
R1#
```

La commande **ping** peut être appelée à la fois en mode privilégié et en mode utilisateur. La commande **ping** peut être utilisée pour confirmer la connectivité de base sur les réseaux AppleTalk, ISO CLNS (service réseau non orienté connexion), IP, Novell, Apollo, VINES, DECnet ou XNS.

L'utilisation d'une commande **ping** étendue indique au routeur d'exécuter une gamme plus étendue d'options de test. Pour utiliser la commande **ping** étendue, entrez **ping** sur la ligne de commande, puis appuyez sur la touche **Entrée** sans saisir d'adresse IP. Des invites de commande vont apparaître chaque fois que vous appuyerez sur la touche **Entrée**. Ces nombreux invites permettent de spécifier davantage d'options que le **ping** standard.

Il est intéressant d'utiliser la commande **ping** lorsque le réseau fonctionne correctement pour voir comment s'exécute cette commande dans des conditions normales et disposer d'un modèle de comparaison lors du dépannage.

Activité de TP

Activité en ligne : Dépannage de la couche 3 au moyen de la commande ping

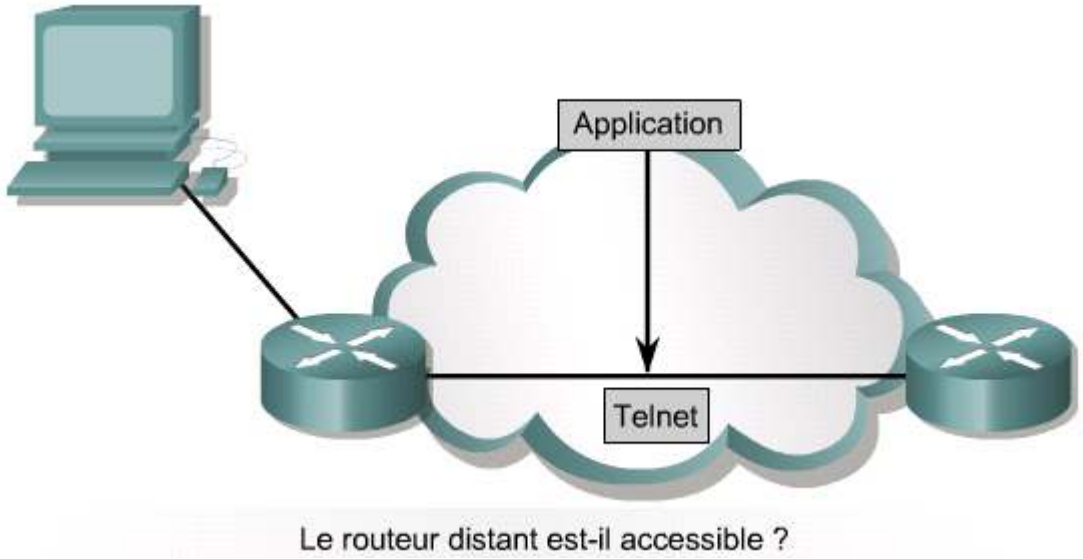
Au cours de ce TP, les étudiants utiliseront la commande ping pour envoyer des requêtes d'écho ICMP à un routeur adjacent.

9.2 Tests réseau

9.2.6 Dépannage de la couche 7 à l'aide de la commande Telnet

L'utilitaire Telnet est un protocole de terminal virtuel qui fait partie de la pile de protocoles TCP/IP. Il permet de vérifier le logiciel de la couche application entre les stations d'origine et de destination. Il s'agit du mécanisme de test le plus complet qui soit. L'utilitaire Telnet est normalement utilisé pour connecter des unités distantes, collecter des informations et exécuter des programmes.

L'application Telnet fournit un terminal virtuel pour la connexion aux routeurs exécutant TCP/IP. Dans le cadre du dépannage, il est utile de vérifier qu'une connexion peut être établie à l'aide de Telnet. Cela prouve qu'au moins une application TCP/IP est capable d'établir une connexion de bout en bout. Une connexion Telnet réussie indique que l'application de couche supérieure, ainsi que les services des couches inférieures, fonctionnent correctement. 1



Si un administrateur peut envoyer une commande Telnet à un routeur mais pas à un autre, vérifiez la connectivité au niveau des couches inférieures. Si la connectivité a été vérifiée, l'échec de Telnet est vraisemblablement dû à des problèmes spécifiques d'adressage, d'attribution de noms ou d'autorisation d'accès. Ces problèmes peuvent exister sur le routeur de l'administrateur ou sur celui que vous avez tenté d'atteindre via Telnet.

Si une commande Telnet vers un serveur donné échoue à partir d'un hôte, essayez de vous connecter à partir d'un routeur et de plusieurs autres unités. Lors des tentatives de connexion via Telnet, si aucune invite de connexion n'apparaît, vérifiez ce qui suit:

- Une recherche DNS inverse sur l'adresse du client peut-elle être trouvée ? De nombreux serveurs Telnet n'autorisent pas les connexions à partir d'adresses IP qui ne disposent pas d'entrées DNS. Il s'agit d'un problème fréquent pour les adresses DHCP dans lesquelles l'administrateur n'a pas ajouté d'entrées DNS pour les groupes DHCP.
- Il est possible qu'une application Telnet ne puisse pas négocier les options appropriées et ne se connecte donc pas. Sur un routeur Cisco, ce processus de négociation peut être visualisé à l'aide de la commande **debugtelnet**.
- Il est possible que l'utilitaire Telnet soit désactivé ou ait été déplacé vers un port autre que 23 sur le serveur de destination.

Activité de TP

Exercice : Dépannage à l'aide des commandes ping et telnet

L'objectif de ce TP est de collecter des informations sur les mises à jour et les protocoles de routage.

Activité de média interactive

Pointer-cliquer : Telnet

À la fin de cette activité, l'étudiant sera en mesure de comprendre Telnet.

9.3 Vue d'ensemble du dépannage des problèmes de routeur

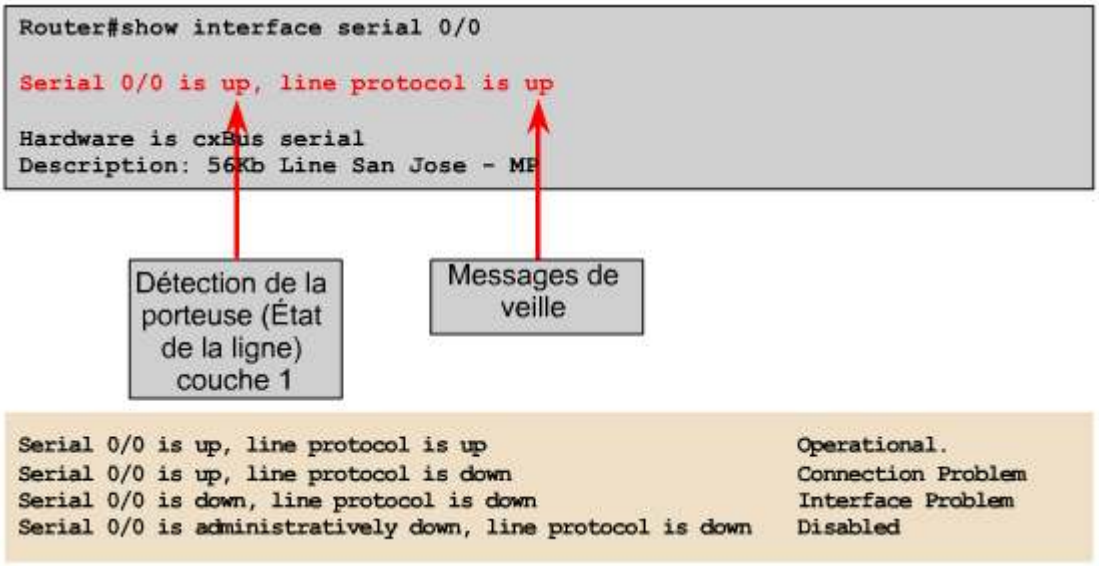
9.3.1 Dépannage de la couche 1 à l'aide de la commande show interfaces

La plate-forme logicielle Cisco IOS contient un jeu complet de commandes de dépannage. Les commandes **show** font partie des commandes plus utilisées. Chaque aspect du routeur peut être observé à l'aide d'une ou de plusieurs commandes **show**. La commande **show** utilisée pour vérifier l'état et les statistiques des interfaces est la commande **show interfaces**. La commande **show interfaces** sans paramètre affiche l'état et les statistiques de toutes les interfaces du routeur. La commande **show interfaces** <interface name> affiche uniquement l'état et les statistiques de l'interface spécifiée. Pour afficher l'état de l'interface Serial 0/0, utilisez la commande **show interfaces serial0/0**.

L'état de deux parties importantes des interfaces est indiqué à l'aide de la commande **show interfaces**. Il s'agit de la partie physique (matérielle) et de la partie logique (logicielle). Celles-ci peuvent être comparées aux fonctions des couches 1 et 2.

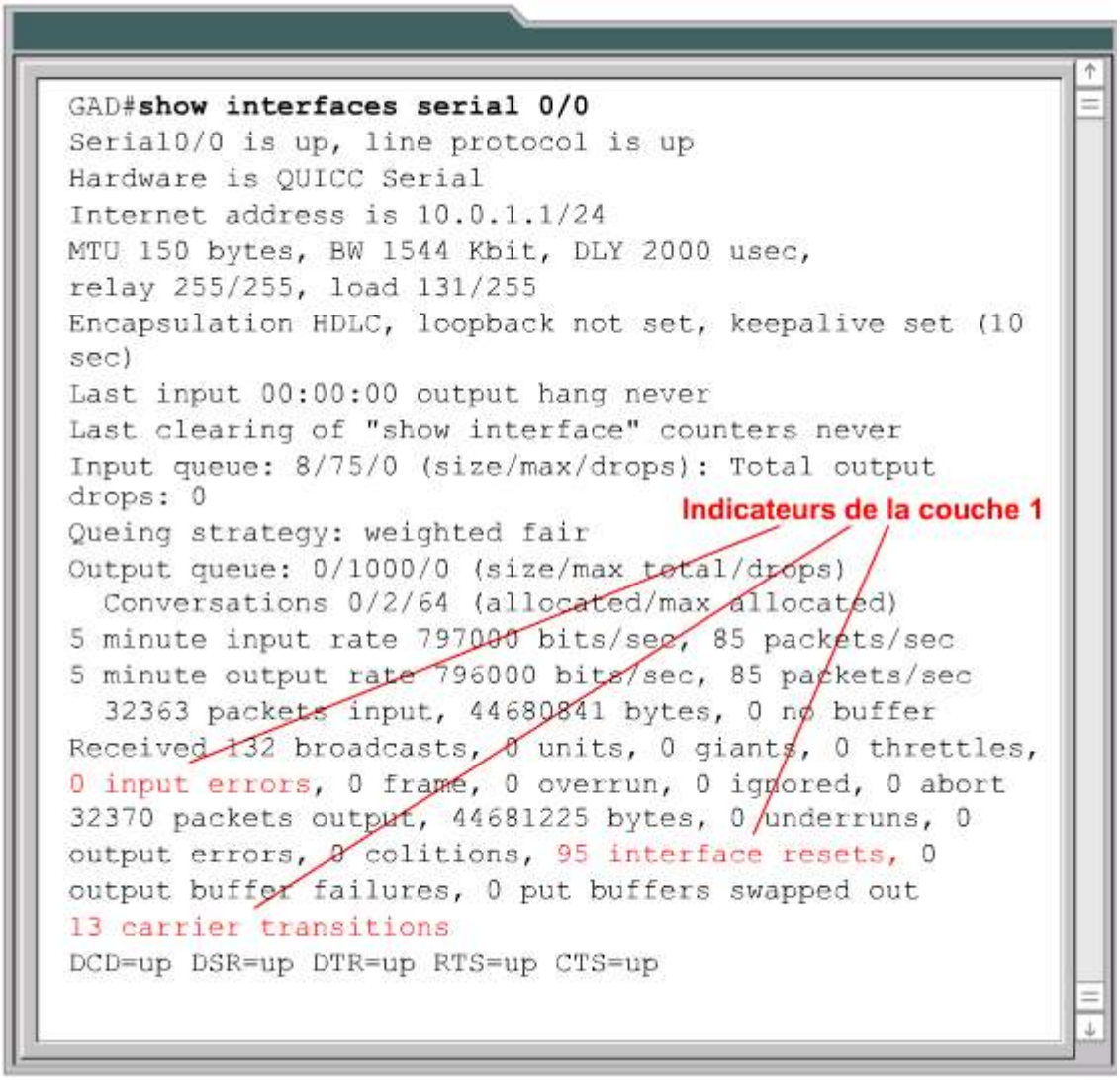
L'état du matériel, comprenant les câbles, les connecteurs et les interfaces, indique l'état de la connexion physique entre les unités. L'état du logiciel indique l'état des messages, tels que les messages de test d'activité, les informations de contrôle et les informations utilisateur, échangés entre des unités voisines. Cela correspond à la condition de protocoles de couche 2 transmis entre deux interfaces de routeurs connectés.

Ces éléments importants sont représentés par l'état du protocole de ligne et de liaison dans les informations affichées par la commande **show interfaces serial**. 1



Le premier paramètre fait référence à la couche matérielle et indique essentiellement si l'interface reçoit le signal « Détection de la porteuse » depuis l'autre extrémité de la connexion. Si la ligne est en panne, il peut exister un problème de câblage, un équipement du circuit peut être hors tension ou présenter un dysfonctionnement, ou une extrémité peut avoir été désactivée par l'administrateur. Si l'interface est en panne sur un plan administratif, elle a été désactivée manuellement dans la configuration.

La commande **`show interfaces serial`** fournit également des informations permettant de diagnostiquer des problèmes de couche 1 qui ne sont pas faciles à détecter. Un nombre croissant de transitions de porteuse sur une liaison série peut indiquer au moins l'un des problèmes suivants: 2



- Des interruptions de ligne dues à des problèmes au niveau du réseau de l'opérateur télécom
- Un commutateur, une unité DSU ou un équipement de routeur défectueux

Si un nombre croissant d'erreurs d'entrée apparaît dans les informations affichées par la commande **`show interfaces serial`**, plusieurs facteurs peuvent être à l'origine de ces erreurs. Certains problèmes sont liés à la couche 1:

- Équipement téléphonique défectueux
- Ligne série parasitée
- Câble inapproprié ou longueur de câble incorrecte
- Câble ou connexion endommagé(e)
- Unité CSU/DSU défectueuse
- Matériel de routeur défectueux

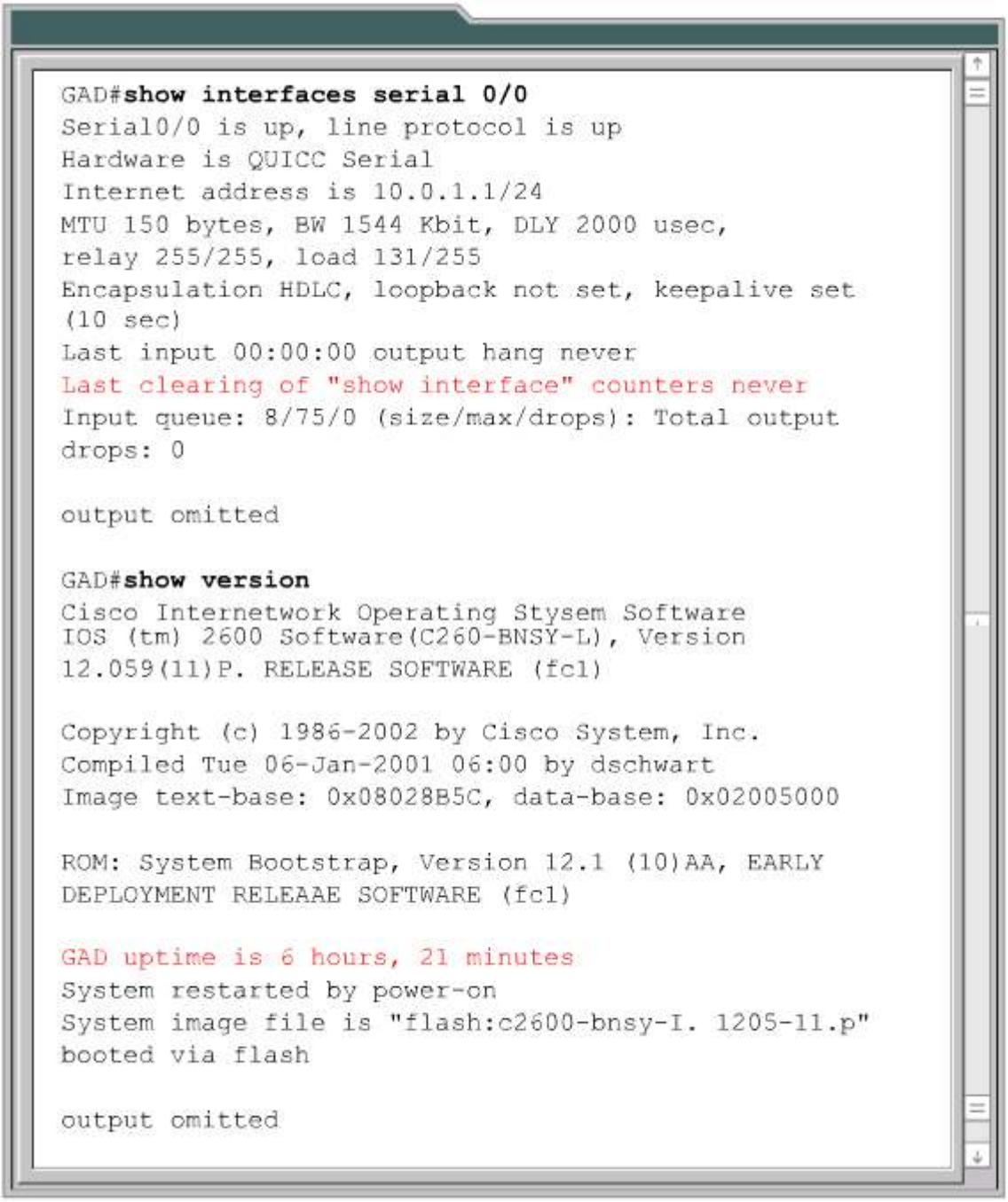
Un autre facteur à examiner est le nombre de réinitialisations d'interface. Celles-ci résultent d'un trop grand nombre de messages de test d'activité. Les problèmes de couche 1 suivants peuvent être à l'origine des réinitialisations d'interface:

- Une ligne incorrecte entraînant des transitions de porteuse
- Un problème matériel au niveau d'une unité CSU/DSU ou d'un commutateur

Si le nombre de transitions de porteuse et de réinitialisations d'interface augmente ou si le nombre d'erreurs d'entrée est élevé alors que les réinitialisations d'interface augmentent, le problème est probablement lié à une liaison incorrecte ou à une unité CSU/DSU défectueuse.

Le nombre d'erreurs doit être interprété par rapport au volume de trafic que le routeur a traité et à la durée de capture des statistiques. Le routeur assure le suivi de statistiques qui fournissent des informations sur l'interface. Les statistiques reflètent

le fonctionnement du routeur depuis son démarrage ou depuis la dernière remise à zéro des compteurs.



```
GAD#show interfaces serial 0/0
Serial0/0 is up, line protocol is up
Hardware is QUICC Serial
Internet address is 10.0.1.1/24
MTU 150 bytes, BW 1544 Kbit, DLY 2000 usec,
relay 255/255, load 131/255
Encapsulation HDLC, loopback not set, keepalive set
(10 sec)
Last input 00:00:00 output hang never
Last clearing of "show interface" counters never
Input queue: 8/75/0 (size/max/drops): Total output
drops: 0

output omitted

GAD#show version
Cisco Internetwork Operating Stysem Software
IOS (tm) 2600 Software(C260-BNSY-L), Version
12.059(11)P. RELEASE SOFTWARE (fc1)

Copyright (c) 1986-2002 by Cisco System, Inc.
Compiled Tue 06-Jan-2001 06:00 by dschwart
Image text-base: 0x08028B5C, data-base: 0x02005000

ROM: System Bootstrap, Version 12.1 (10)AA, EARLY
DEPLOYMENT RELEAAE SOFTWARE (fc1)

GAD uptime is 6 hours, 21 minutes
System restarted by power-on
System image file is "flash:c2600-bnsy-I. 1205-11.p"
booted via flash

output omitted
```

Si les informations affichées par la commande **`show interfaces`** indiquent que les compteurs ne sont jamais remis à zéro, utilisez la commande **`show version`** pour rechercher depuis quand le routeur est en service.

Utilisez la commande **`clear counters`** pour remettre les compteurs à zéro. Ces compteurs devraient toujours être effacés après résolution d'un problème d'interface. La remise à zéro donne une meilleure image de l'état actuel du réseau et permet de vérifier que le problème a bien été corrigé.

Activité de TP

Activité en ligne : Dépannage de la couche 1 au moyen de la commande show interface

Au cours de ce TP, les étudiants vont vérifier que la liaison physique Serial 0/0 est active, remettre les compteurs d'interface à zéro, puis vérifier de nouveau l'interface pour déterminer les changements survenus après la remise à zéro.

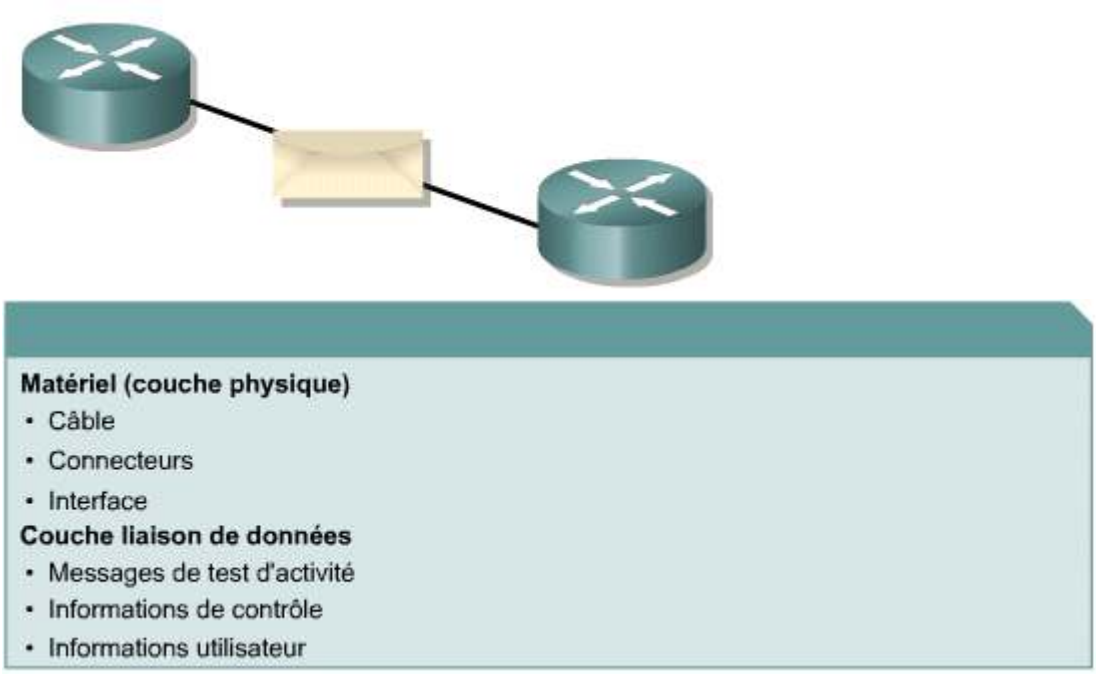
La commande **`show interfaces`** est peut-être l'outil le plus important pour découvrir les problèmes de couche 1 et 2 avec le routeur. Le premier paramètre (ligne) fait référence à la couche physique. Le deuxième paramètre (protocole) indique si les processus de l'IOS qui contrôlent le protocole de ligne considèrent l'interface comme utilisable. Cela dépend de la réception ou non des messages de test d'activité. Les messages de test d'activité sont des messages envoyés par une unité du réseau à une autre pour lui indiquer que le circuit virtuel existant entre les deux est toujours actif. Si l'interface manque trois messages de test d'activité consécutifs, le protocole de ligne est considéré comme inactif.

Lorsque la ligne est inactive, le protocole est toujours inactif, car il n'existe aucun média utilisable pour le protocole de couche 2. Cela est particulièrement vrai lorsque l'interface est en panne à cause d'un problème matériel et lorsqu'elle a été désactivée par un administrateur.

Si l'interface est active et que le protocole de ligne est désactivé, un problème de couche 2 existe. Les causes possibles sont les suivantes:

- Aucun message de test d'activité (keepalives)
- Aucune fréquence d'horloge (clock rate)
- Aucune correspondance au niveau du type d'encapsulation

La commande **`show interfaces serial`** doit être utilisée après configuration d'une interface série pour vérifier les modifications et s'assurer que l'interface est opérationnelle.



Activité de média interactive

Glisser-Positionner : Commande show interface *interface*

À la fin de cette activité, l'étudiant sera en mesure de comprendre la commande show interface *interface*.

9.3 Vue d'ensemble du dépannage des problèmes de routeur

9.3.3 Dépannage à l'aide de la commande show cdp

Le protocole CDP (Cisco Discovery Protocol) annonce des informations sur les unités à ses voisins directs, notamment les adresses MAC et IP, ainsi que les interfaces de sortie.

```
GAD#show cdp neighbors
Capability Codes: R - Router, T - Bridge, B - Sourse, Route Bridge,
                  S - Switch, H- Host, I - IGMP, r- Repeater

Device ID     LocalInterface   Holdtime   Capability   Platform    Port ID
3350-srvs     Fas 0/0          153        R S I        WS-C3550-2  Fas 0/1
Cyberspace    ser 0/1          171        R            3640        Ser 1/1
004096581e28 Fas 0/0           150                     AIR-AP350   fec0
0040965716a5 Fas 0/0           152                     AIR-AP350   fec
BHM           Ser 0/0          137        R            2601        Ser 0/0
access1       Fas 0/2          162        R            2511        Eth 0
```

Les informations affichées par la commande **show cdp neighbors** contiennent des informations sur les unités voisines Cisco directement connectées. 1Ces informations sont utiles pour le débogage des problèmes de connectivité. Si un problème de câblage est suspecté, activez les interfaces avec la commande **no shutdown**, puis exécutez la commande **show cdp neighbors detail** avant toute autre configuration. La commande affiche les détails relatifs à une unité spécifique, tels que les interfaces actives, l'ID de port et l'équipement. La version de la plate-forme logicielle Cisco IOS exécutée sur les unités distantes apparaît également.

Si la couche physique fonctionne correctement, toutes les autres unités Cisco directement connectées doivent être affichées. L'absence d'unité connue reflète probablement un problème au niveau de la couche 1.

Le protocole CDP présente un problème de sécurité. La quantité d'informations fournies par CDP est tellement vaste que ce protocole peut être à l'origine d'une défaillance au niveau de la sécurité. 2Pour des raisons de sécurité, CDP doit être configuré uniquement sur des liaisons entre des unités Cisco, et désactivé sur les ports ou les liaisons utilisateur qui ne sont pas gérés localement.

```
GAD#show cdp neighbors detail
-------------------------
Device ID: 33 50- srvs
Entry address(es): IP address: 192.168.119.245
Platform: cisco WS-C3550-24, Capabilities: Router Switch IGMP
Interface: Ethernet0, Port ID (outgoing port): FastEthernet0/1
Holdtime: 179 sec

Version:
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Version 12.1(8) EA1c, RELEASE
   SOFTWARE
(fc1)
Copyright (c) 1986_2002 by cisco Systems, Inc.
Compiled Fri 15-Feb-02 10:50 by antonino
```

Activité de TP

Activité en ligne : Protocole CDP (Cisco Discovery Protocol)

Au cours de ce TP, les étudiants vont utiliser le protocole CDP pour obtenir des informations sur les unités Cisco voisines.

9.3 Vue d'ensemble du dépannage des problèmes de routeur

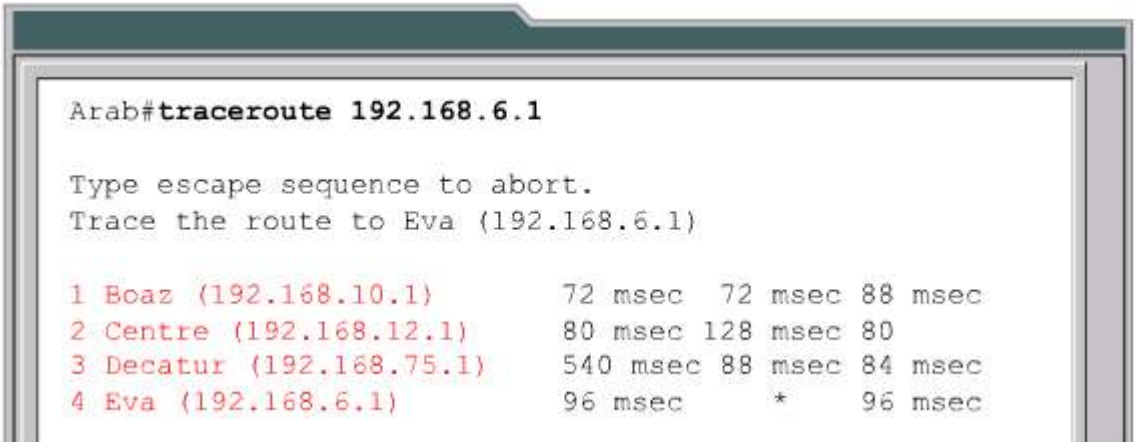
9.3.4 Dépannage à l'aide de la commande traceroute

La commande **traceroute** est utilisée pour découvrir les routes que les paquets empruntent lors du déplacement vers leur destination. L'utilitaire Traceroute peut également être utilisé pour aider à tester la couche réseau (couche 3) saut par saut et pour fournir des références pour les performances.

La commande **traceroute** est souvent référée comme étant la commande **trace** dans le matériel de référence. Cependant, la syntaxe exacte de la commande est **traceroute**.

Les informations affichées par la commande **traceroute** indiquent également le saut au niveau duquel le problème est survenu. Pour chaque routeur du chemin, une ligne de sortie, générée sur le terminal, indique l'adresse IP de l'interface ayant reçu les données. Si un astérisque (*) apparaît, le paquet a échoué. En recherchant le dernier saut correct dans les informations affichées par la commande **traceroute** et en le comparant à un schéma de l'interréseau, il est possible d'identifier la zone problématique.

Traceroute fournit également des informations indiquant les performances relatives des liaisons. Le temps de parcours aller-retour (RTT) est le temps nécessaire pour envoyer un paquet et obtenir une réponse. 1Cette information est utile pour avoir une idée approximative du délai sur la liaison. Ces chiffres ne sont pas suffisamment précis pour être utilisés pour une évaluation de performance exacte. Toutefois, ces informations peuvent être capturées et utilisées dans le cadre du dépannage futur de l'interréseau.



Notez que l'unité qui reçoit la commande **traceroute** doit savoir comment envoyer la réponse à l'unité ayant généré la commande **traceroute**. Pour que les données **traceroute** ou **ping** circulent correctement entre les routeurs, il doit exister des routes connues dans les deux directions. L'échec d'une réponse n'est pas toujours synonyme de problème, car les messages ICMP ont pu être limités en débit ou filtrés au niveau du site hôte. Ceci est particulièrement vrai sur Internet.

Traceroute envoie une séquence de datagrammes UDP (User Datagram Protocol) à partir du routeur vers une adresse de port non valide sur l'hôte distant. Pour la première séquence de trois datagrammes envoyée, la valeur du champ Durée de vie est définie sur un. Avec cette valeur, le datagramme est temporisé au niveau du premier routeur sur le chemin. Ce routeur répond ensuite en envoyant un message ICMP de dépassement du délai indiquant que le datagramme a expiré.

Trois autres messages UDP sont à présent envoyés, avec cette fois une valeur de durée de vie réglée sur 2. En conséquence, le deuxième routeur renvoie des messages ICMP de dépassement du délai. Ce processus se poursuit jusqu'à ce que les paquets atteignent réellement leur destination ou que le TTL maximum ait été atteint. La valeur maximale par défaut de TTL pour traceroute est 30.

Étant donné que ces datagrammes tentent d'accéder à un port non valide sur l'hôte de destination, des messages ICMP de port inaccessible sont renvoyés à la place du message ICMP de dépassement du délai. Le fait que le port soit inaccessible est signalé au programme traceroute et le processus prend fin.

Activité de TP

Exercice : Dépannage à l'aide de la commande traceroute

L'objectif de ce TP est d'utiliser la commande traceroute ou tracert pour vérifier que la couche réseau entre le routeur

source, le routeur de destination et chaque routeur du chemin fonctionne correctement.

9.3 Vue d'ensemble du dépannage des problèmes de routeur

9.3.5 Dépannage des problèmes de routage

Les commandes **show ip protocols** et **show ip route** affichent des informations sur les protocoles de routage et sur la table de routage. Les informations affichées par ces commandes peuvent être utilisées pour vérifier la configuration du protocole de routage.

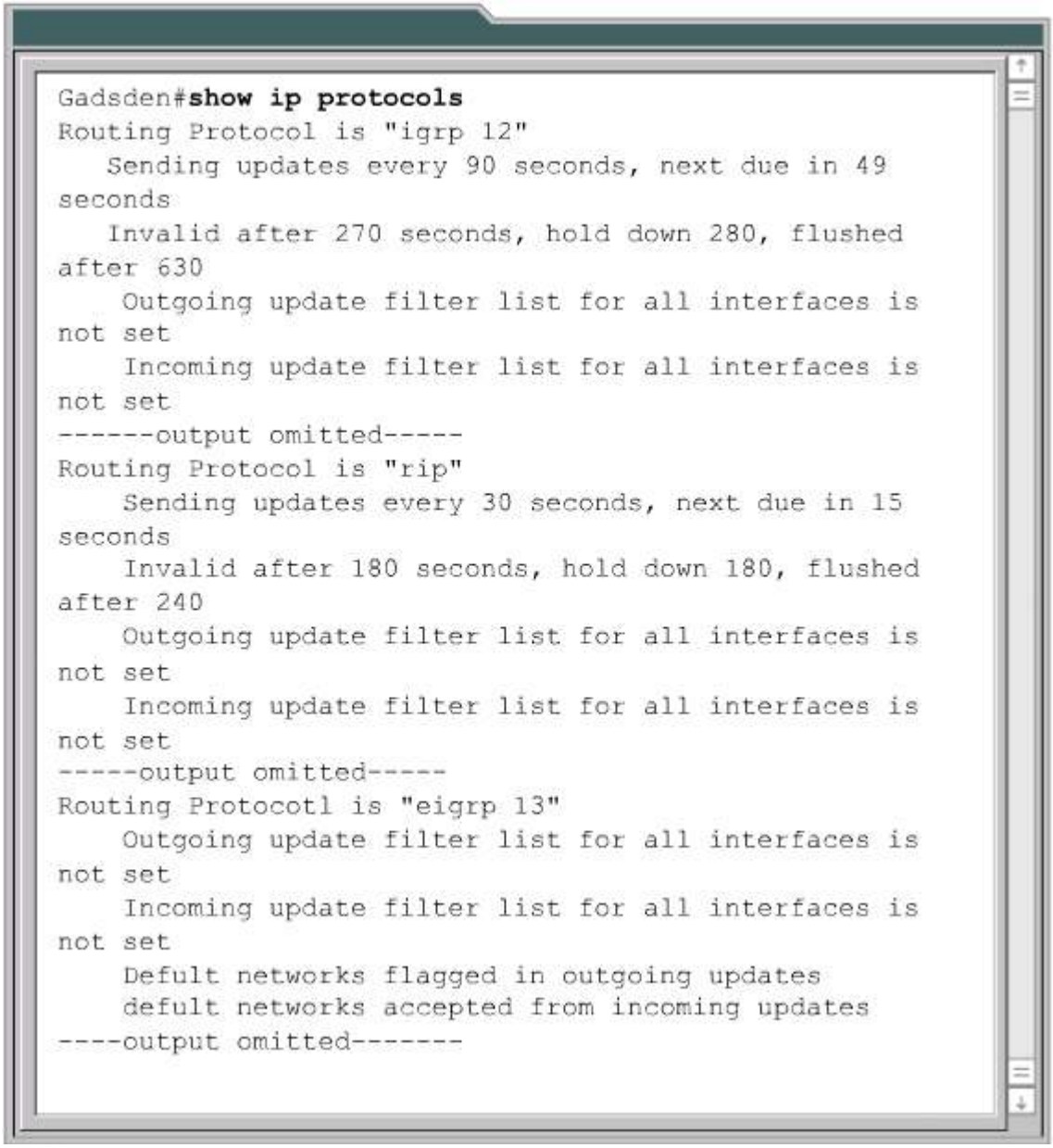
La commande **show ip route** est peut-être la commande la plus importante pour le dépannage des problèmes de routage. Cette commande affiche le contenu de la table de routage IP. Les informations affichées par la commande **show ip route** indiquent les entrées pour tous les réseaux et sous-réseaux connus, et la manière dont ces informations ont été apprises. 1

```
Gadsden#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP,
       M - mopble, B - BGP, D - EIGRP,
       EX - EIGRP external, 0 - OSPF,
       IA - OSPF inter area,
       E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EGP, I - IS-IS,
       L1 - IS-IS level-1,
       L2 - IS-IS level-2, * - candidate default
       U - per-user static rout, o - ODR

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D   10.0.0.0/8 is a summary, 18:14:42, Null0
C   10.0.1.0/25 is directly connected, Serial0/0
R   192.168.40.0/24 [120/1] via 10.0.1.2, 00:00:10,
  Serial0/0
                    [120/1] via 172.16.01, 00:00:11,
  FastEthernet0/0
I   192.168.32.0/24 [100/1600] via 172.16.0.1, 18:14:45,
  FastEthernet0/0
D   192.168.56.0/24 [90/409600] via 172.16.0.1,
  18:14:45, FastEthernet0/0
D    192.168.57.0/24 [90/409600] via 172.16.0.1,
  18:14:45, FastEthernet0/0
R    192.168.48.0/24 [120/1] via 10.0.1.2, 00:00:16,
  Serial0/0
                     [120/1] via 172.16.0.1, 00:00:16,
  FastEthernet0/0
----(output omitted)----
C 172.16.0.0/16 is directly connected, FastEthernet0/0
```

En cas de problème pour atteindre un hôte dans un réseau donné, vous pouvez utiliser les informations affichées par la commande **show ip route** pour vérifier que le routeur dispose d'une route pour ce réseau.

Si les informations affichées par la commande **`show ip route`** ne contiennent pas les routes apprises attendues ou n'indiquent aucune route apprise, il est possible que le problème soit lié à l'absence d'échange d'informations de routage. Dans ce cas, utilisez la commande **`show ip protocols`** sur le routeur pour rechercher une erreur de configuration du protocole de routage.

La commande **`show ip protocols`** affiche des données de protocole de routage IP pour la totalité du routeur. Cette commande peut être utilisée pour identifier les protocoles configurés, les réseaux annoncés, les interfaces envoyant des mises à jour et les sources des mises à jour de routage. Les informations affichées par la commande **`show ip protocols`** indiquent également les compteurs, les filtres, le récapitulatif et la redistribution des routes, ainsi que des paramètres propres à chaque protocole de routage activé sur le routeur. Lorsque plusieurs protocoles de routage sont configurés, les informations relatives à chaque protocole sont répertoriées dans une section séparée.



```
Gadsden#show ip protocols
Routing Protocol is "igrp 12"
   Sending updates every 90 seconds, next due in 49
seconds
   Invalid after 270 seconds, hold down 280, flushed
after 630
    Outgoing update filter list for all interfaces is
not set
    Incoming update filter list for all interfaces is
not set
------output omitted-----
Routing Protocol is "rip"
    Sending updates every 30 seconds, next due in 15
seconds
    Invalid after 180 seconds, hold down 180, flushed
after 240
    Outgoing update filter list for all interfaces is
not set
    Incoming update filter list for all interfaces is
not set
-----output omitted-----
Routing Protocotl is "eigrp 13"
    Outgoing update filter list for all interfaces is
not set
    Incoming update filter list for all interfaces is
not set
    Defult networks flagged in outgoing updates
    defult networks accepted from incoming updates
----output omitted-------
```

Les informations affichées par la commande **`show ip protocols`** peuvent être utilisées pour diagnostiquer une multitude de problèmes de routage, notamment l'identification d'un routeur soupçonné de fournir des informations de routage erronées. Il peut être utilisé pour confirmer la présence des protocoles attendus, des réseaux annoncés et des unités de routage voisines. Comme avec tout processus de dépannage, l'identification du problème est difficile voire impossible si aucune documentation n'indique ce qui est normalement attendu.

Activité de TP

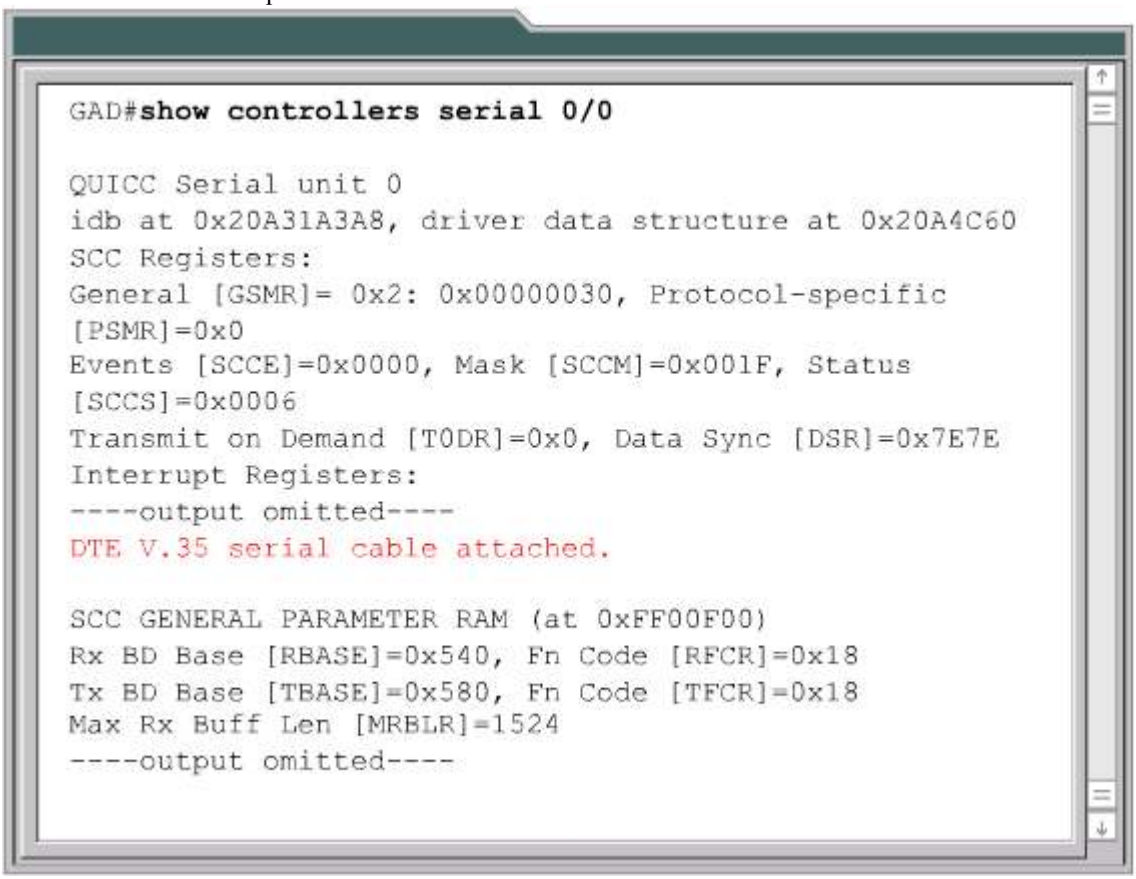
Exercice : Dépannage des problèmes de routage avec **show ip route** et **show ip protocols**

L'objectif de ce TP est d'utiliser les commandes **show ip route** et **show ip protocols** pour diagnostiquer un problème de configuration du routage.

9.3 Vue d'ensemble du dépannage des problèmes de routeur

9.3.6 Dépannage à l'aide de la commande show controllers

Très souvent, la configuration et le dépannage sur les routeurs sont effectués à distance lorsqu'il n'est pas possible de contrôler physiquement les connexions des routeurs. La commande show controllers sert à déterminer le type de câble connecté sans avoir à inspecter les câbles. 1



```
GAD#show controllers serial 0/0

QUICC Serial unit 0
idb at 0x20A31A3A8, driver data structure at 0x20A4C60
SCC Registers:
General [GSMR]= 0x2: 0x00000030, Protocol-specific
[PSMR]=0x0
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status
[SCCS]=0x0006
Transmit on Demand [T0DR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
----output omitted----
DTE V.35 serial cable attached.

SCC GENERAL PARAMETER RAM (at 0xFF00F00)
Rx BD Base [RBASE]=0x540, Fn Code [RFCR]=0x18
Tx BD Base [TBASE]=0x580, Fn Code [TFCR]=0x18
Max Rx Buff Len [MRBLR]=1524
----output omitted----
```

En examinant les informations affichées par la commande show controllers, vous pouvez déterminer le type de câble détecté par le contrôleur. Ces informations sont utiles pour repérer une interface série sans câble, un type de câble incorrect ou un câble défectueux.

La commande **show controllers serial 0/0** interroge le circuit intégré, ou puce de contrôleur, qui contrôle les interfaces série et affiche des informations sur l'interface physique série 0/0. Le résultat varie d'une puce de contrôleur à une autre. Le résultat varie d'une puce de contrôleur à une autre. Même au sein d'un même type de routeur, différentes puces de contrôleur peuvent être utilisées.

Quel que soit le type de contrôleur, la commande **show controllers** génère une quantité importante d'informations. Mis à part le type de câble, la plus grande partie de ces informations sont des détails techniques internes concernant l'état de la puce du contrôleur. Sans connaissance spécifique sur les circuits intégrés, ces informations sont peu utiles.

Activité de média interactive

Pointer-cliquer : Tests réseau

À la fin de cette activité, l'étudiant sera en mesure de comprendre le processus de test d'un réseau

Activité de TP

Activité en ligne : Dépannage au moyen de la commande **show controllers serial**

Au cours de ce TP, les étudiants vont utiliser la commande show controllers pour connaître le type de câble connecté à l'interface série.

9.3 Vue d'ensemble du dépannage des problèmes de routeur

9.3.7 Présentation des commandes debug

Les commandes **debug** permettent d'identifier précisément les problèmes de protocole et de configuration. La commande **debug** est utilisée pour afficher des événements et des données dynamiques. Étant donné que les commandes **show** n'affichent que des informations statiques, elles fournissent une représentation historique du fonctionnement du routeur. L'utilisation des informations affichées par la commande **debug** procure des informations sur les événements en cours sur le routeur. Ces événements peuvent concerner le trafic sur une interface, les messages d'erreur générés par des nœuds sur le réseau, les paquets de diagnostic propres à un protocole et d'autres données utiles pour le dépannage. 1

```
GAD#debug ip eigrp
IP-EIGRP Route Events debugging is on
GAD#show debug
IP route IP_EIGRP Route debugging is on
```

Le résultat dynamique de la commande **debug** peut nuire aux performances, car il crée des surcharges sur le processeur susceptibles d'interrompre le fonctionnement normal du routeur. C'est pourquoi la commande **debug** doit être utilisée avec parcimonie. Utilisez les commandes **debug** pour examiner certains types de trafic ou des problèmes spécifiques après avoir envisagé plusieurs causes possibles. Les commandes **debug** doivent être utilisées pour localiser des problèmes et non pour surveiller le fonctionnement normal du réseau. 2

```
GAD#debug ?
aaa                 AAA Authentication, Authorization and
                    Accounting
access-expression   Boolean access expression
all                 Enable all debugging
arp                 IP ARP and HP Probe transactions
async               Async interface information
broadcast           MAC broadcast packets
callback            Call back activity
cdp                 CDP information
----output omitted----
bridge              Transparet Bridging
telnet              Incoming telnet connctions
tftp                TFTP packets
token               Token Ring information
tunnel              Generic Tunnel Interface
v120                V120 information
x25                 X.25 information
```

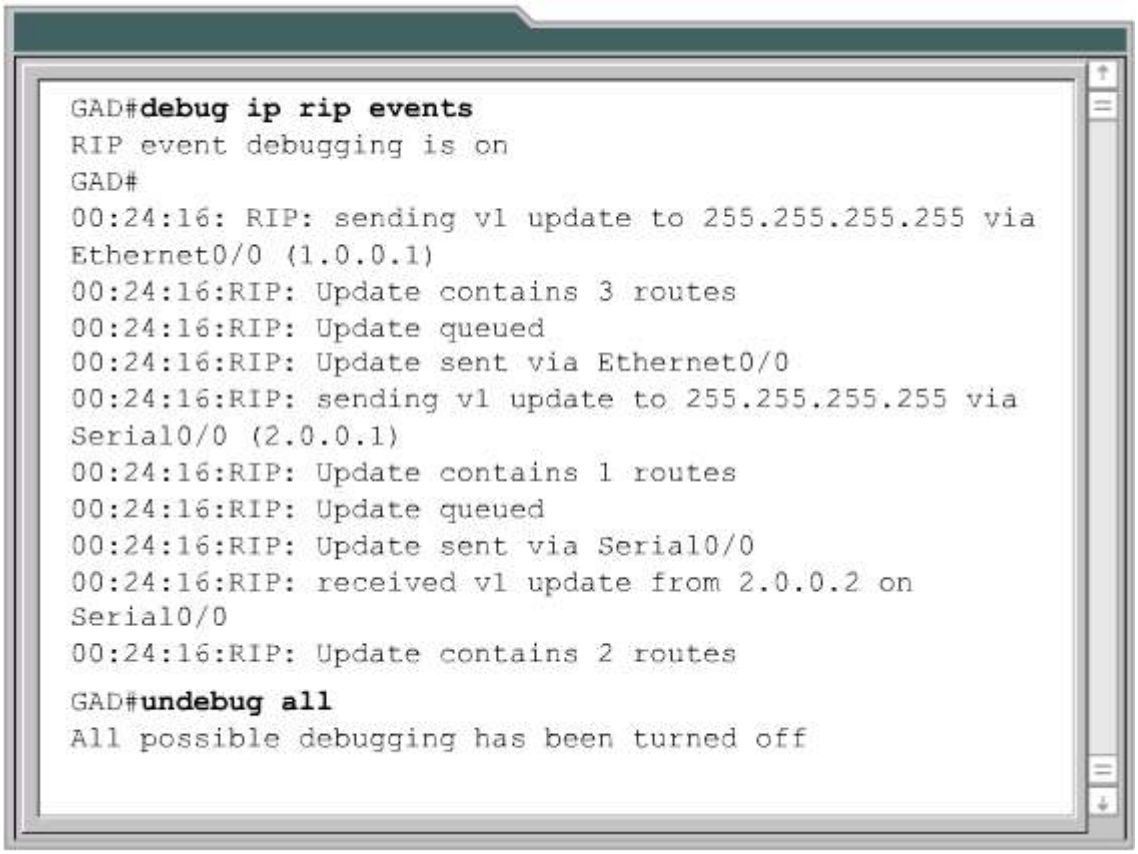
AVERTISSEMENT ::

La commande **debugall** doit être utilisée avec modération, car elle peut interrompre le fonctionnement du routeur.

Par défaut, le routeur envoie les informations affichées par la commande **debug** et les messages système à la console. Si une session telnet est utilisée pour examiner le routeur, les informations affichées par la commande **debug** et les messages système peuvent être redirigés vers le terminal distant. Cela est réalisé au sein de la session telnet par la saisie de la commande **terminal monitor**. La sélection de commandes **debug** à partir d'une session telnet nécessite une attention toute particulière. Vous ne devez sélectionner aucune commande **debug** susceptible d'engendrer un trafic supplémentaire générant l'affichage d'informations supplémentaires. Dans ce cas, le trafic au sein de la session telnet risque de saturer rapidement la liaison ou le routeur risque d'épuiser une ou plusieurs ressources. Pour empêcher cette récursion du trafic, respectez la règle suivante : ne déboguez jamais une activité sur le port sur lequel la session est établie.

Le résultat des différentes commandes **debug** varie. Certaines commandes génèrent fréquemment de nombreuses lignes tandis que d'autres produisent une ligne ou deux à intervalles de quelques minutes. 3 4

```
GAD#debug ip packet detail
10w6d:  TCP src=1075, dst=80, seg=785595392,
ack=3448593899 win=64240 ACK
10w6d:IP:s=192.168.120.145(Ethernet0/0), d=192.168.119.9
(Ethernet0/0), g=192.168.119.9, len 60, forward
10w6d:  TCP src=1075, dst=80, seg=785595392,
ack=3448599739 win=64240 ACK
10w6d:IP:s=192.168.120.145(Ethernet0/0), d=192.168.119.9
(Ethernet0/0), g=192.168.119.9, len 60, forward
10w6d:  TCP src=1075, dst=80, seg=785595392,
ack=3448604710 win=64240 ACK
10w6d:IP:s=192.162.168.120.145(Ethernet0/0),
d=192.168.119.9(Ethernet0/0), g=192.168.119.9, len 60,
forward
10w6d:  TCP src=1075, dst=80, seg=785595392,
ack=3448593899 win=64240 ACK
10w6d:IP:s=10.1.1.81(Serial0/0), d=224.0.0.10, len
        64, rcvd 2, proto=88
10w6d:IP:s=210.107.197.105(Serial0/0),
d=192.168.119.255, len 1028, access denied
10w6d:  ICMP type=8, code=0
10w6d:IP:s=10.1.1.82(loac1), d=224.0.0.10(Serial0/0),
len 22, sending broad/multicast, proto=88
10w6d:IP s=0.0.0.0(Ethernet0/0), d=255.255.255.255, len
590,rcvd 2
10w6d:   UDP src=68, dst=67
10w6d:IP s=192.168.120.50(Ethernet0/0),
d=192.168.120.255(Ethernet0/0), len 243, rcvd 3
GAD#undebug all
All possible debugging has been turned off
```



La commande **timestamps** est un autre service de la plate-forme logicielle Cisco IOS qui amplifie l'utilité des informations affichées par la commande **debug**. Cette commande place un horodatage sur un message de déboguage. Cette information indique l'heure de l'événement de déboguage et le temps écoulé entre plusieurs événements.

Cela est très utile quand il faut dépanner des problèmes intermittents. En horodatant l'affichage, une forme récurrente est souvent reconnue. Cela aide à isoler la source du problème. Cela évite aussi aux techniciens de regarder attentivement pendant des heures l'affichage de déboguage.

La commande suivante configure un horodatage qui indique l'heure de l'affichage (sous la forme heure:minute:seconde), le temps écoulé depuis la dernière mise en marche du routeur ou depuis l'exécution d'une commande de rechargement:

```
GAD(config)#service timestamps debug uptime
```

Ainsi, l'affichage est ainsi très utile pour déterminer le délai écoulé entre deux événements. Le délai écoulé depuis le dernier rechargement sert de référence pour déterminer l'intervalle de temps écoulé depuis la dernière occurrence de l'événement de déboguage. Ce délai peut être trouvé avec la commande **show version**.

Une utilisation plus pratique de l'horodatage est d'afficher l'heure et la date d'arrivée d'un événement. Cela simplifie la détermination de la dernière occurrence d'un événement de déboguage. Cette possibilité est fournie par l'option **datetime**:

```
GAD(config)#service timestamps debug datetime localtime
```

Il faut bien noter que cette commande n'est utile que si l'horloge du routeur a été réglée. Sinon, les informations d'horodatage inclues dans l'affichage de déboguage ne correspondront pas à l'heure exacte. Pour s'assurer que les informations d'horodatages sont correctes, l'horloge du routeur doit être réglée sur l'heure exacte en utilisant la commande suivante, entrée en mode privilégié:

```
GAD#clock set 15:46:00 3 May 2004
```

Sur certaines plates-formes Cisco, l'horloge du routeur n'est pas maintenue sur batterie. Il faudra donc régler l'horloge du routeur après chaque rechargement ou panne d'alimentation électrique.

```
GAD(config)#service timestamps debug uptime
```

La commande **no debug all** ou **undebug all** désactive tous les messages de diagnostic. Pour désactiver une commande **debug** en particulier, utilisez la forme **no** de la commande. Par exemple, si la surveillance du protocole RIP a été activée avec la commande **debug ip rip**, vous pouvez la désactiver avec la commande **no debug ip rip**. Pour afficher ce qui est analysé par une commande **debug**, utilisez la commande **show debugging**.

Activité de TP

Exercice : Dépannage des problèmes de routage avec la commande debug

L'objectif de ce TP est d'utiliser un processus de dépannage OSI systématique pour le diagnostic des problèmes de routage.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Commande **show ip route**
- Détermination de la passerelle de dernier recours
- Détermination de la route entre la source et la destination
- Détermination de la distance administrative de la route
- Détermination de la métrique de la route
- Détermination du saut suivant de la route
- Détermination de la dernière mise à jour de la route
- Observation de chemins multiples vers une destination
- Utilisation d'une approche structurée du dépannage
- Test sur la base des couches OSI
- Dépannage de la couche 1 à l'aide des témoins lumineux
- Dépannage de la couche 3 à l'aide de la commande ping
- Dépannage de la couche 7 à l'aide de la commande Telnet
- Dépannage de la couche 1 à l'aide de la commande **show interfaces**
- Dépannage de la couche 2 à l'aide de la commande **show interfaces**
- Dépannage à l'aide de la commande show **cdp**
- Dépannage à l'aide de la commande **traceroute**
- Dépannage des problèmes de routage avec **show ip route** et **show ip protocols**
- Dépannage à l'aide de la commande **show controllers serial**
- Dépannage à l'aide des commandes **debug**

- L'une des principales fonctions d'un routeur est de déterminer le meilleur chemin vers une destination donnée. Un routeur " apprend " les chemins, également appelés routes, à partir de la configuration manuelle d'un administrateur ou à partir d'autres routeurs par le biais de protocoles de routage.
- Une table de routage contient la liste des meilleures routes disponibles. Les routeurs utilisent la table de routage pour prendre des décisions concernant la transmission des paquets.
- Les commandes **telnet** et **ping** permettent de tester un réseau.
- La plate-forme logicielle Cisco IOS contient un jeu complet de commandes de dépannage. Les commandes **show** figurent parmi les plus utilisées. Chaque aspect du routeur peut être observé à l'aide d'une ou de plusieurs commandes **show**.

Vue d'ensemble

Les routeurs utilisent les informations d'adresse de protocole IP (Internet Protocol) dans un en-tête de paquet IP pour déterminer l'interface vers laquelle le paquet doit être commuté pour se rapprocher de sa destination. Étant donné que le protocole IP ne fournit aucun service pour garantir que le paquet atteint réellement sa destination, il est considéré comme un

protocole non fiable et non orienté connexion qui assure l'acheminement « au mieux » des données. Si des paquets sont abandonnés en route, arrivent dans le mauvais ordre ou sont transmis plus rapidement que le récepteur ne peut les accepter, IP ne peut pas corriger le problème seul. Pour résoudre ces problèmes, IP a besoin du protocole TCP (Transmission Control Protocol). Ce module décrit TCP et ses fonctions et présente UDP, un autre protocole important de couche 4.

Chaque couche du modèle de référence OSI a des fonctions variées. Ces fonctions sont indépendantes des autres couches. Chaque couche s'attend à recevoir des services de la couche immédiatement inférieure et fournit des services spécifiques à la couche immédiatement supérieure. Les couches application, présentation et session du modèle OSI, qui sont toutes considérées comme faisant partie de la couche application du modèle TCP/IP, accèdent aux services de la couche transport par le biais d'entités logiques appelées ports. Ce module présente le concept de port, et explique l'importance des ports et des numéros de port dans les réseaux de données.

À la fin de ce module, les étudiants doivent être en mesure de:

- Décrire le protocole TCP et sa fonction
- Décrire la synchronisation et le contrôle de flux TCP
- Décrire le fonctionnement du protocole UDP et les processus correspondants
- Identifier les numéros de port les plus courants
- Décrire des conversations multiples entre des hôtes
- Identifier les ports utilisés pour les services et les clients
- Décrire la numérotation des ports et les ports bien connus
- Comprendre les différences et les relations entre les adresses MAC, les adresses IP et les numéros de port

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
10.1	Fonctionnement du protocole TCP
10.2	Vue d'ensemble des ports de la couche transport

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
		• Utilisation du modèle OSI en tant que guide pour le dépannage systématique de réseau	• Évaluation du processus de communication TCP/IP et de ses protocoles associés

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
		• Utilisation du modèle OSI en tant que guide pour le dépannage systématique de réseau	

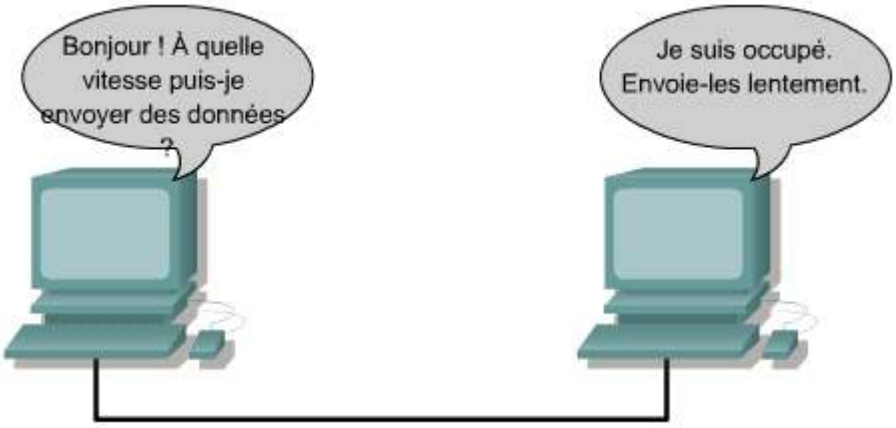
Ce module porte sur les objectifs suivants de l'examen INTRO 640-821 :

Conception et support	Mise en œuvre et fonctionnement	Technologie
		• Description de l'impact des protocoles associés à TCP/IP sur la communication des hôtes

10.1 Fonctionnement du protocole TCP

10.1.1 Fonctionnement du protocole TCP

Les adresses IP permettent d'acheminer des paquets entre des réseaux. Toutefois, IP ne garantit en aucun cas leur livraison finale. La couche transport assure avec fiabilité le transport et la régulation du flux de données depuis la source jusqu'à la destination. Pour cela, des fenêtres glissantes et des numéros de séquence sont utilisés, parallèlement à un processus de synchronisation qui garantit que chaque hôte est prêt à communiquer. 1



Pour comprendre la fiabilité et le contrôle du flux, imaginez un étudiant qui fait l'apprentissage d'une nouvelle langue pendant un an. Imaginez ensuite que cet étudiant visite le pays dans lequel cette langue est parlée couramment. Lorsqu'il communique dans cette langue, l'étudiant doit demander à la personne de répéter chacune de ses phrases (fiabilité) et de parler lentement, pour s'assurer de comprendre chacun des mots (contrôle de flux). La couche transport, couche 4 du modèle OSI, fournit ces services à la couche 5 au moyen de TCP.

10.1 Fonctionnement du protocole TCP

10.1.2 Synchronisation ou échange en trois étapes

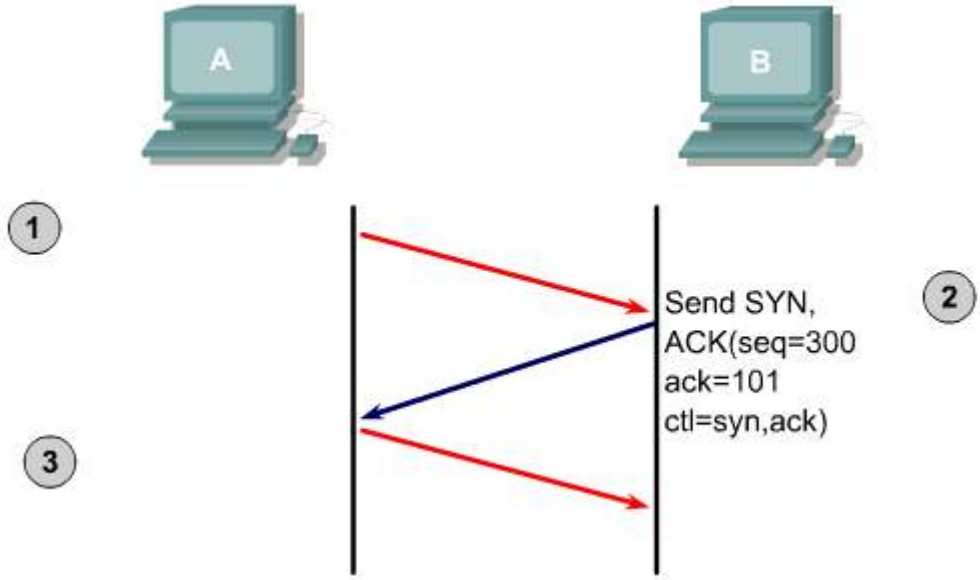
Le protocole TCP est orienté connexion. Avant de transmettre des données, les deux hôtes exécutent un processus de synchronisation pour établir une connexion virtuelle pour chaque session entre les hôtes. Ce processus de synchronisation permet de vérifier que les deux hôtes sont prêts pour la transmission des données et permet aux unités de déterminer les numéros de séquence initiaux pour cette session. Ce processus est appelé échange en trois étapes. Il s'agit d'un processus en trois étapes qui établit une connexion virtuelle entre les deux unités. Il est important de bien noter que cet échange en trois étapes est initié par l'hôte client. Pour établir une session TCP, l'hôte client va utiliser le numéro de port bien connu du service qu'il désire contacter et qui est fourni par l'hôte serveur.

- Dans la première étape, l'hôte qui initie l'échange (le client) envoie un paquet de synchronisation (drapeau SYN positionné) pour amorcer une connexion. Ceci indique que dans ce segment, pour cette session, un paquet a un numéro de séquence initial valide «x». Le bit SYN positionné dans l'en tête indique qu'il s'agit d'une demande de connexion. Le bit SYN est contenu dans le champ de code de l'en tête du segment TCP. Le numéro de séquence est un champ de 32 bits de l'en tête du segment TCP. 1

0	4	10	16	24	31
Port source			Port de destination		
Numéro de séquence					
Numéro d'accusé de réception					
HLEN	Réservé	Bits de code	Fenêtre		
Somme de contrôle			Pointeur d'urgence		
Options (le cas échéant)				Remplissage	
Données					
...					

La structure des champs d'un segment TCP contient un en-tête TCP suivi de données. Les segments servent à établir les connexions, ainsi qu'à transporter les données et les accusés de réception.

- Dans la deuxième étape, l'autre hôte reçoit le paquet, enregistre le numéro de séquence «x» donné par le client, et répond par un accusé de réception (drapeau ACK positionné). Le bit de contrôle ACK positionné indique que le champ du numéro d'accusé de réception contient un numéro d'accusé de réception valide. Le drapeau ACK est un constitué d'un bit contenu dans le champ de code de l'en tête du segment TCP et le numéro d'accusé de réception est un champ de 32 bits de l'en tête du segment TCP. Quand une connexion est établie, le drapeau ACK est positionné dans tous les segments tout au long de la session. Le champ d'accusé de réception contient le prochain numéro de séquence attendu par l'hôte (x+1). Un accusé de réception de «x+1» signifie que l'hôte a bien reçu tous les octets jusqu'à l'octet «x» compris et qu'il s'attend à recevoir l'octet «x+1». L'hôte initie aussi une session en retour. Celle-ci intègre dans le segment TCP son propre numéro de séquence initial «y» et positionne le bit SYN.



- Dans la troisième étape, l'hôte à l'origine de la demande de connexion répond par un simple accusé dont la valeur est «y+1», c'est-à-dire le numéro de séquence adressé en retour par le deuxième host plus 1 (numéro de séquence de l'hôte B + 1). Ceci indique qu'il a reçu l'accusé de réception précédent et finalise le processus de connexion.

Il est important de comprendre que les numéros de séquence initiaux contribuent à démarrer la communication entre les deux unités. Ils servent de numéros de référence de départ entre les deux unités. Les numéros de séquence donnent à chaque hôte le moyen d'envoyer un accusé de réception de sorte que le récepteur sache que l'émetteur répond bien à la demande de connexion appropriée.

Activité de média interactive

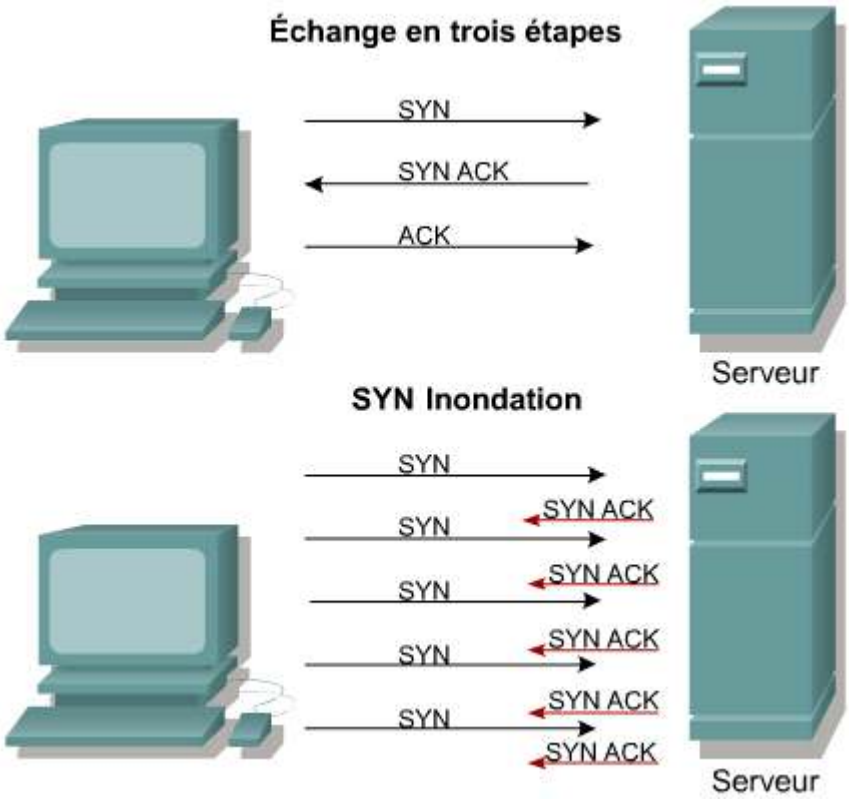
Glisser-Positionner : Synchronisation TCP

À la fin de cette activité, l'étudiant sera en mesure de comprendre la synchronisation TCP.

10.1 Fonctionnement du protocole TCP
10.1.3 Attaques par déni de service

Les attaques par déni de service sont destinées à refuser des services à des hôtes légitimes qui tentent d'établir des connexions. Les attaques par déni de service sont utilisées par les pirates pour bloquer les réponses système. L'inondation SYN est un type d'attaque par déni de service. Elle exploite le processus normal d'échange en trois étapes et oblige les unités cible à envoyer un accusé de réception à des adresses source, qui ne complètent pas l'échange en trois étapes.

L'échange en trois étapes débute lorsque le premier hôte envoie un paquet de synchronisation (SYN). Le paquet SYN inclut l'adresse IP source et l'adresse IP de destination. Ces informations d'adresse sont utilisées par le récepteur pour renvoyer le paquet d'accusé de réception à l'unité émettrice. 1



Dans une attaque par déni de service, le pirate lance une synchronisation mais « usurpe » l'adresse IP source. On parle de « spoofing » lorsque l'unité réceptrice répond à une adresse IP inexistante et inaccessible, puis est placée dans un état d'attente jusqu'à recevoir l'accusé de réception final de l'unité émettrice. La requête d'attente est placée dans une file d'attente de connexion ou dans une zone d'attente en mémoire. Cet état d'attente oblige l'unité attaquée à consommer des ressources système, telles que la mémoire, jusqu'à ce que le délai de connexion expire. Les pirates inondent l'hôte attaqué de fausses requêtes SYN, l'obligeant à utiliser toutes ses ressources de connexion, ce qui l'empêche de répondre aux requêtes de connexion légitimes.

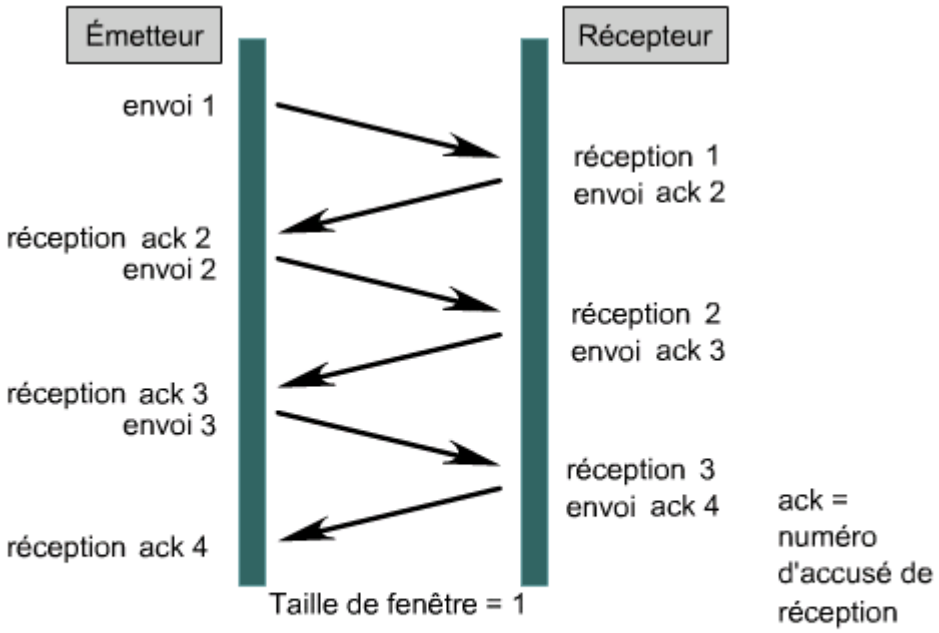
Pour se protéger contre ces attaques, les administrateurs système peuvent diminuer le délai d'attente de connexion et augmenter la taille de la file d'attente de connexion. Il existe également des logiciels capables de détecter ce type d'attaque et de mettre en place des mesures de protection.

10.1 Fonctionnement du protocole TCP
10.1.4 Fenêtrage et taille de fenêtre

La quantité de données à transmettre est souvent trop volumineuse pour être envoyée dans un seul segment de données. Dans ce cas, les données doivent être divisées en segments plus petits pour permettre une meilleure transmission. TCP est responsable de la répartition de ces données en segments. Cela peut être comparé à la manière que les petits enfants sont nourris. Leur nourriture est souvent coupée en plus petits morceaux mieux adaptés à leur bouche. De plus, l'unité réceptrice peut ne pas être capable de recevoir les données aussi rapidement que la source les envoie, car elle peut être occupée par d'autres activités ou simplement parce que l'émetteur est plus puissant.

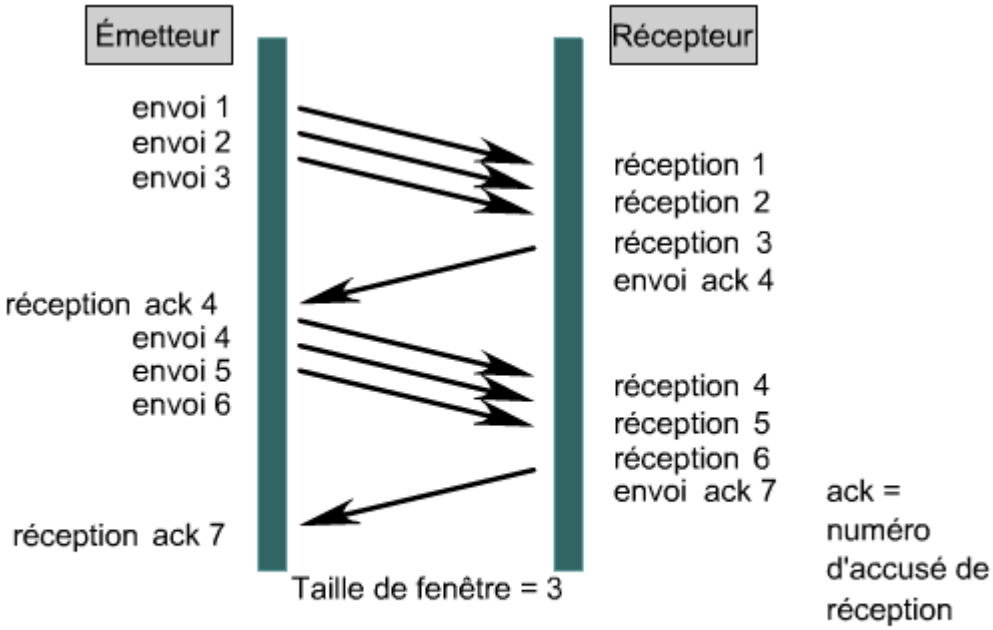
Une fois les données segmentées, elles doivent être transmises à l'unité de destination. L'un des services fournis par TCP est le contrôle du flux, qui régule la quantité de données envoyées au cours d'une période de transmission donnée. Le processus de contrôle du flux est appelé fenêtrage.

La taille de fenêtre définie la quantité de données qui peut être transmise à la fois avant que la destination ne réponde par un accusé de réception. Quand un hôte a transmis un nombre d'octets correspondant à la taille de la fenêtre, il doit attendre un accusé de réception lui indiquant que ces données ont bien été reçues, avant de pouvoir envoyer d'autres données. Par exemple, si la taille de la fenêtre est égale à 1, un octet ne peut pas être envoyé avant que l'accusé de réception de l'octet précédent n'ait été reçu. 1



Ceci a été simplifié pour l'exemple. Les tailles de fenêtres habituelles sont bien plus grandes, en général plusieurs milliers d'octets.

TCP utilise le fenêtrage pour ajuster de façon dynamique la taille des transmissions. Les équipements négocient une taille de fenêtre pour autoriser la transmission d'un nombre défini d'octets avant d'émettre un accusé de réception. 2



Ceci a été simplifié pour l'exemple. Les tailles de fenêtres habituelles sont bien plus grandes, en général plusieurs milliers d'octets.

Ce processus d'ajustement dynamique de la taille de la fenêtre augmente la fiabilité. La taille de la fenêtre peut être modulée en fonction des accusés de réception.

Activité de média interactive

Associer : Fenêtrage

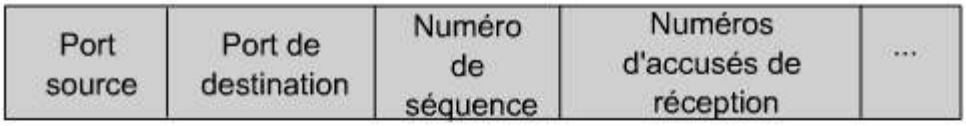
À la fin de cette activité, l'étudiant sera en mesure de comprendre le fenêtrage.

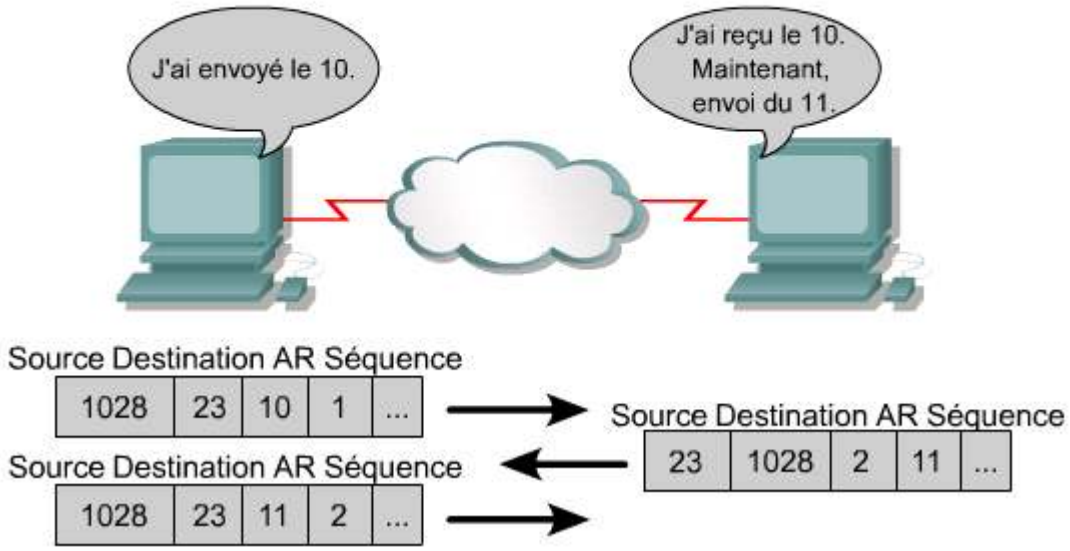
10.1 Fonctionnement du protocole TCP

10.1.5 Numéros de séquence

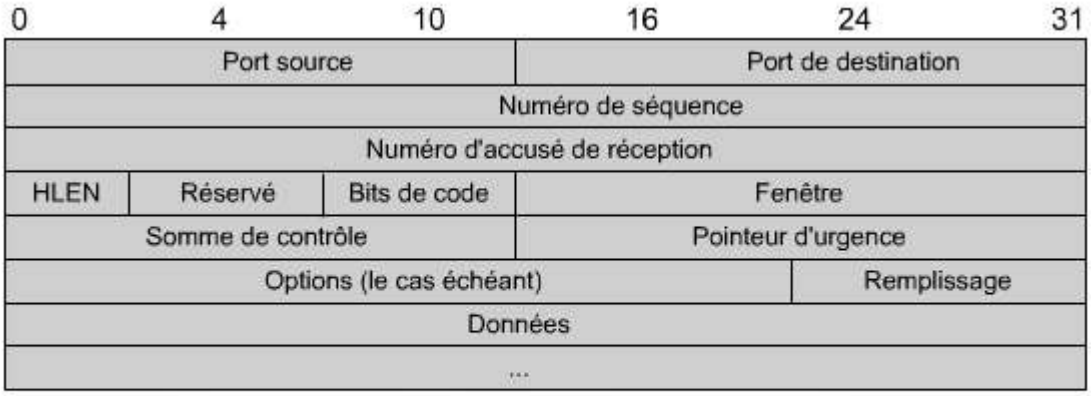
TCP sépare les données en segments. Les segments de données sont ensuite transmis par l'émetteur au récepteur, après synchronisation et négociation d'une taille de fenêtre qui détermine le nombre d'octets pouvant être transmis en une seule fois. Une fois que toutes les données ont été reçues, les segments de données transmis doivent être assemblés. Il n'existe aucune garantie concernant l'ordre d'arrivée des données. TCP applique des numéros de séquence aux segments de données transmis, de sorte que le récepteur soit capable d'assembler correctement les octets dans leur ordre d'origine. Si des segments TCP arrivent de manière désordonnée, les segments peuvent être assemblés dans le mauvais ordre. Les numéros de séquence indiquent à l'unité de destination l'ordre correct dans lequel placer les octets lorsqu'ils sont reçus.

Ces numéros de séquence servent également de numéros de référence, de sorte que le récepteur sache s'il a reçu la totalité des données. Ils identifient également les données manquantes, de sorte que l'émetteur puisse les transmettre de nouveau. [1]





Les performances sont ainsi accrues car l'émetteur n'a besoin de retransmettre que les segments manquants au lieu du jeu de données complet.



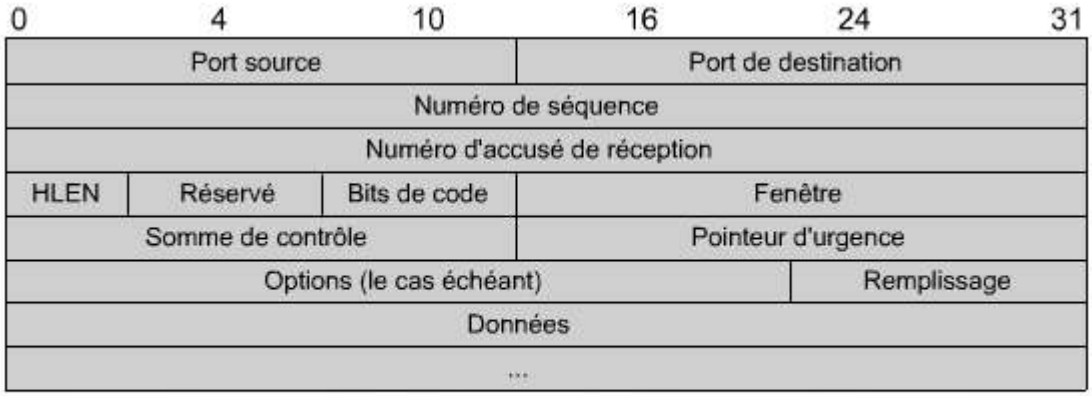
La structure des champs d'un segment TCP contient un en-tête TCP suivi de données. Les segments servent à établir les connexions, ainsi qu'à transporter les données et les accusés de réception.

Chaque segment TCP est numéroté avant la transmission. 2 Dans la syntaxe des segments, notez que le port de destination est suivi du numéro de séquence. Au niveau de la station de réception, le protocole TCP utilise les numéros de séquence pour assembler les segments en un message complet. Si un numéro de séquence est absent de la série, le segment correspondant est retransmis.

10.1 Fonctionnement du protocole TCP

10.1.6 Accusés de réception positifs

L'accusé de réception est une étape commune du processus de synchronisation qui comprend les fenêtres glissantes et le séquençage des données. Dans un segment TCP, le champ du numéro de séquence est suivi du champ du numéro d'accusé de réception, également appelé champ de code. 1



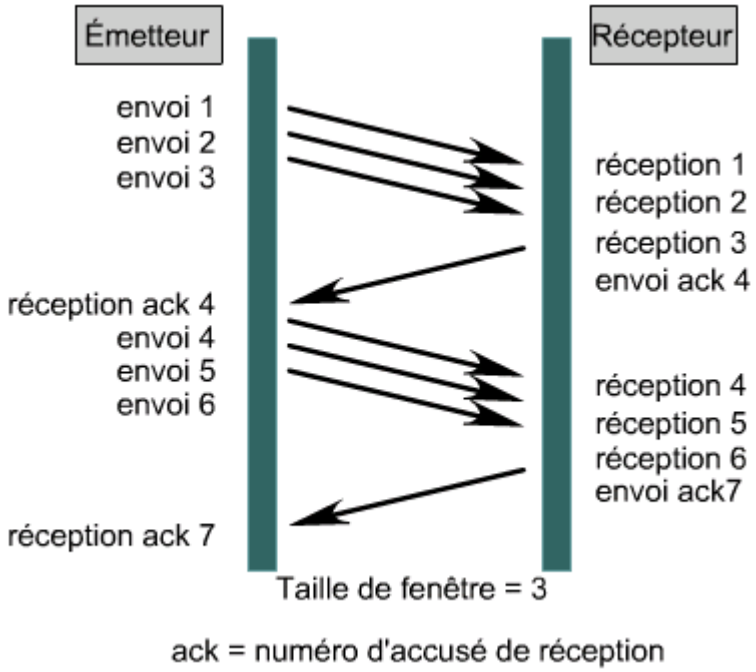
La structure des champs d'un segment TCP contient un en-tête TCP suivi de données. Les segments servent à établir les connexions, ainsi qu'à transporter les données et les accusés de réception.

Ce champ est l'endroit où s'effectue le suivi des octets transmis et reçus.

Le protocole IP présente un problème de fiabilité, car il n'existe aucune méthode pour vérifier que les segments de données ont réellement atteint leur destination. Les segments de données peuvent donc être transmis continuellement sans que leur réception soit réellement confirmée. TCP utilise une technique de retransmission et d'accusé de réception pour contrôler le flux de données et confirmer l'arrivée des données.

La technique PAR est utilisée par de nombreux protocoles comme gage de fiabilité. Selon la technique PAR, la source envoie un paquet, démarre un compteur et attend un accusé de réception avant d'envoyer le paquet suivant, dans la même session. Si le compteur arrive à expiration avant que la source n'ait reçu un accusé de réception, celle-ci retransmet le paquet et redémarre le compteur. L'accusé de réception est fourni par la valeur du numéro d'accusé de réception et par le drapeau ACK positionné, qui sont inclus dans l'en tête TCP. Le protocole TCP utilise des accusés de réception prévisionnels dans lesquels le numéro de l'accusé de réception indique le prochain octet attendu dans la session TCP.

Le fenêtrage est un mécanisme de contrôle de flux selon lequel l'unité source doit recevoir un accusé de réception de la part de la destination après transmission d'une certaine quantité de données. Si la taille de fenêtre est de trois, l'unité source peut envoyer trois octets à l'unité de destination. Elle doit ensuite attendre un accusé de réception. Si l'unité de destination reçoit les trois octets, elle envoie un accusé de réception à la source, qui peut alors envoyer trois autres octets. Si, pour une raison quelconque, l'unité de destination ne reçoit pas les trois octets, parfois en raison d'un dépassement de capacité des tampons, elle n'envoie pas d'accusé de réception. Lorsqu'elle ne reçoit pas d'accusé de réception, l'unité source sait que les octets doivent être transmis de nouveau, à un débit plus lent. Cette réduction de la taille de la fenêtre permet à l'unité de réception d'avoir moins d'octets à traiter dans ces tampons avant que d'autres données arrivent. Cela réduit, de façon efficace, la vitesse de transmission entre les hôtes, mais cela augmente la fiabilité de la communication. 2



Activité de TP

Exercice : Sessions d'hôtes actives multiples

Ce TP illustre l'utilisation des ports sur un hôte unique connecté à un routeur.

Activité de média interactive

Interactivité : Fenêtres glissantes TCP

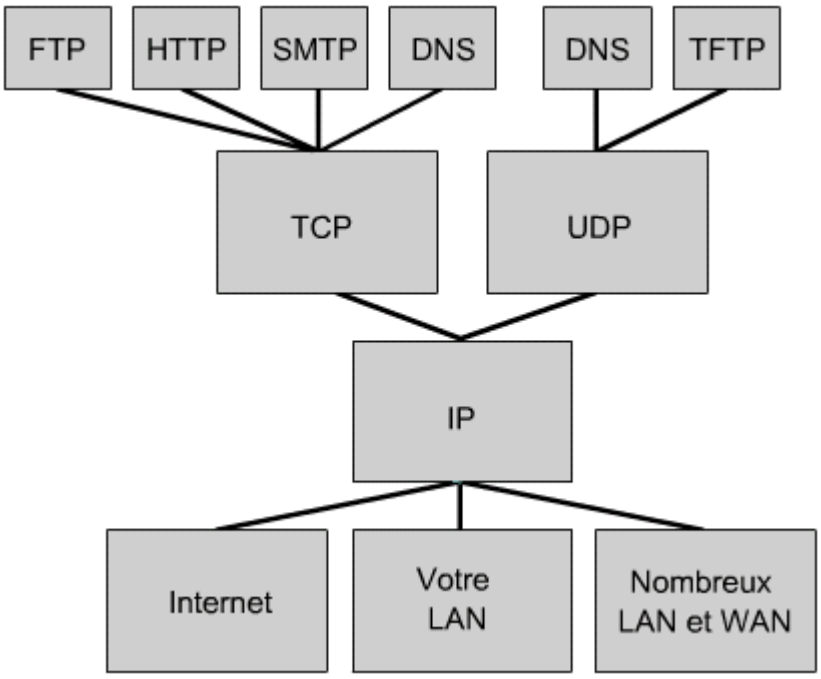
À la fin de cette activité, l'étudiant sera en mesure de comprendre la taille de fenêtre.

10.1 Fonctionnement du protocole TCP

10.1.7 Fonctionnement du protocole UDP

La pile de protocoles TCP/IP contient de nombreux protocoles, chacun devant effectuer un travail précis. Le protocole IP permet une transmission non orientée connexion au niveau de la couche 3 dans un interréseau. Le protocole TCP permet une transmission de paquets orientée connexion et fiable au niveau de la couche 4 du modèle OSI. Le protocole UDP permet une transmission de paquets non orientée connexion et sans garantie de remise conforme au niveau de la couche 4 du modèle OSI.

Les protocoles TCP et UDP utilisent IP comme protocole de couche 3 sous-jacent. De plus, TCP et UDP sont utilisés par divers protocoles de la couche application. TCP fournit des services d'applications, tels que FTP, HTTP, SMTP et DNS. UDP est le protocole de la couche transport utilisé par DNS, TFTP, SNMP et DHCP. 1



TCP doit être utilisé lorsque les applications ont besoin de garantir qu'un paquet arrive intact, dans le bon ordre et non dupliqué. La surcharge associée à la confirmation d'arrivée d'un paquet est parfois problématique lors de l'utilisation de TCP. Les applications n'ont pas toutes besoin de garantir l'arrivée du paquet de données. Elles utilisent donc la technique de livraison la plus rapide et non orientée connexion fournie par le protocole UDP. Le protocole UDP standard, décrit dans la spécification RFC 768, est un protocole simple qui échange des segments sans accusé de réception, ni distribution garantie.

Nombre de bits	16	16	16	16	16
	Port source	Port de destination	Longueur	Somme de contrôle	Données...

Les segments UDP ne contiennent pas de champs de séquence ou d'accusé de réception.

Le protocole UDP n'utilise ni fenêtrage, ni accusé de réception. Par conséquent, les protocoles de couche application doivent assurer la détection des erreurs. 2Le champ du port source est un champ facultatif utilisé uniquement lorsque des informations ont besoin d'être renvoyées à l'hôte émetteur. Lorsqu'un routeur de destination reçoit une mise à jour de routage, le routeur source n'envoie aucune requête, et le routeur de destination n'a donc pas besoin de renvoyer des informations à la source. Le champ du port de destination indique l'application à laquelle UDP doit transmettre les données. Une requête DNS d'un hôte vers un serveur DNS utilise le port de destination 53, numéro de port UDP pour DNS. Le champ Longueur identifie le nombre d'octets dans le segment UDP. Le champ Somme de contrôle UDP est facultatif mais peut être utilisé pour garantir que les données n'ont pas été endommagées pendant la transmission. Pour leur transport sur le réseau, les segments UDP sont encapsulés dans le paquet IP.

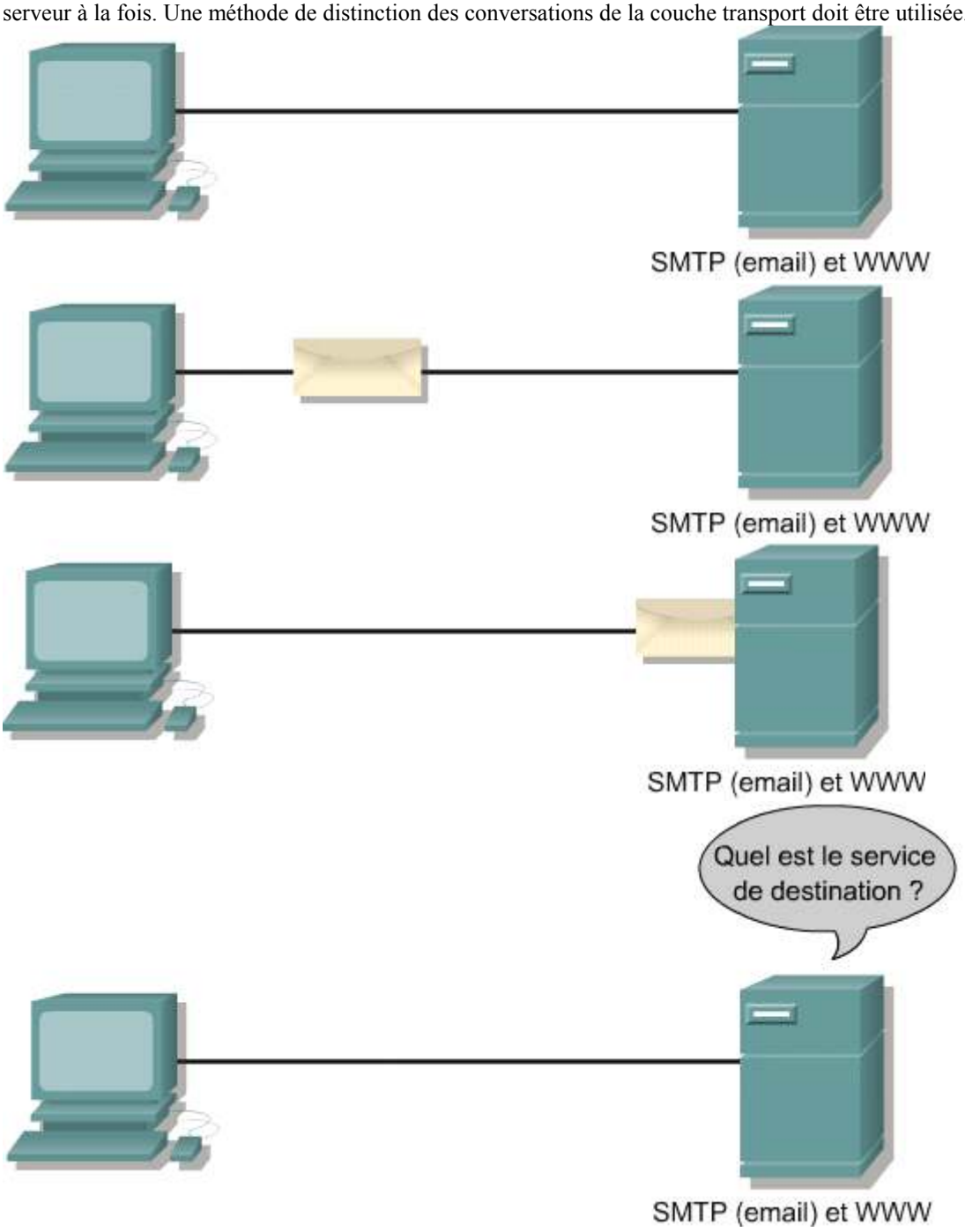
Une fois qu'un segment UDP arrive à l'adresse IP de destination, il doit exister un mécanisme permettant à l'hôte récepteur de déterminer l'application de destination exacte. Les ports de destination sont utilisés à cet effet. Si un hôte exécute à la fois les services TFTP et DNS, il doit être capable de déterminer le service dont le segment UDP entrant a besoin. Le champ Port de destination dans l'en-tête UDP détermine l'application à laquelle un segment UDP est destiné.

10.2 Vue d'ensemble des ports de la couche transport

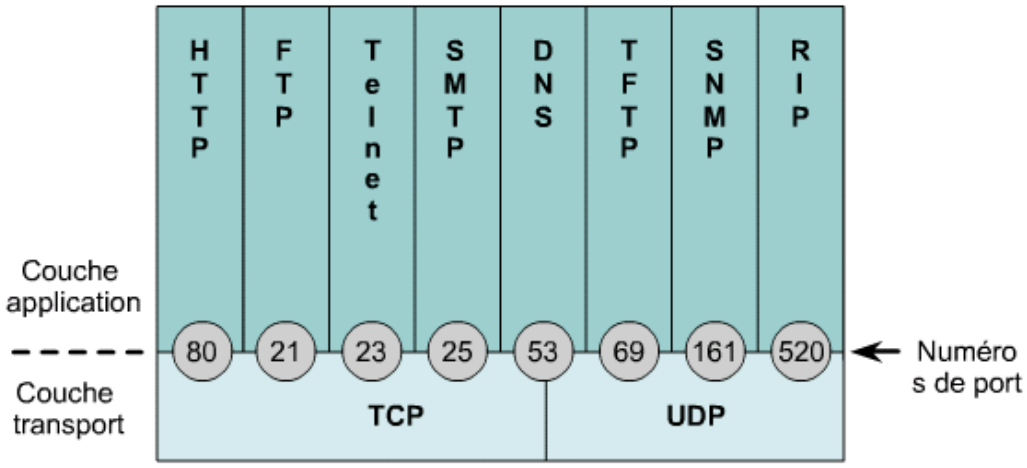
10.2.1 Conversations multiples entre hôtes

À un moment donné, des milliers de paquets fournissant des centaines de services différents traversent un réseau moderne. Dans la plupart des cas, des serveurs fournissent une multitude de services, créant des problèmes uniques pour l'adressage des paquets. Si un serveur exécute à la fois SMTP et HTTP, il utilise le champ Port de destination pour déterminer le service demandé par la source. La source ne peut pas créer un paquet destiné uniquement à l'adresse IP du serveur, car la destination ne serait pas en mesure de déterminer le service demandé. 1Un numéro de port doit être associé à la conversation entre les hôtes pour garantir que le paquet atteint le service approprié sur le serveur. Sans moyen de distinguer les différentes

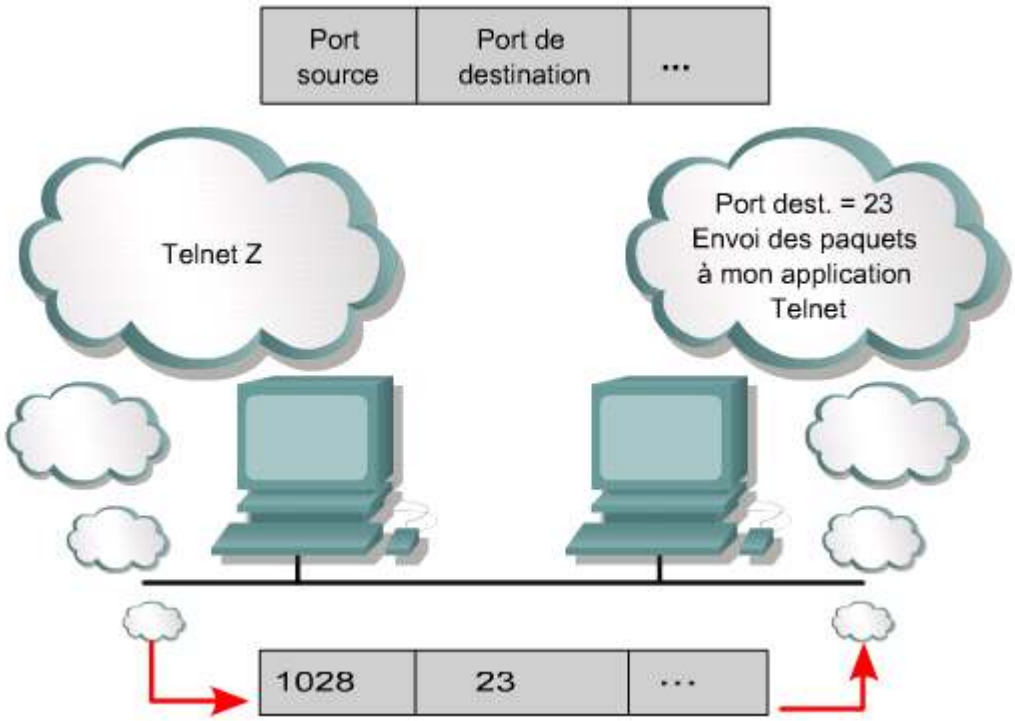
conversations, le client serait incapable d'envoyer un message électronique tout en ouvrant une page Web, à l'aide d'un serveur à la fois. Une méthode de distinction des conversations de la couche transport doit être utilisée.



Les hôtes exécutant TCP/IP associent des ports au niveau de la couche transport à certaines applications. Les numéros de port servent à distinguer les différentes conversations qui circulent simultanément sur le réseau. Les numéros de port sont nécessaires lorsqu'un hôte communique avec un serveur exécutant plusieurs services. Les protocoles TCP et UDP utilisent des numéros de port ou de socket pour transmettre des informations aux couches supérieures.



Les développeurs d'applications ont convenu d'utiliser les numéros de port bien connus qui sont définis dans la spécification RFC 1700. Toute conversation destinée à l'application FTP utilise le numéro de port standard 21. 2 Les conversations qui ne visent pas des applications ayant des numéros de port bien connus se voient attribuer des numéros aléatoires sélectionnés à l'intérieur d'une plage donnée. Ces numéros sont utilisés en tant qu'adresses source et de destination dans le segment TCP. 3



Les plages attribuées aux numéros de port sont les suivantes:

- Les 1023 premiers ports sont des ports bien connus.
- Les ports enregistrés sont compris entre 1024 et 49151.
- Les ports compris entre 49152 et 65535 sont des ports dits dynamiques ou privés.

Les systèmes initiant des requêtes de communication se servent des numéros de port afin de sélectionner les applications appropriées. Les numéros de port source pour ces requêtes sont affectés de manière dynamique par l'hôte émetteur et sont généralement supérieurs à 1023. Les numéros de port compris entre 0 et 1023 sont considérés publics et sont contrôlés par l'IANA (Internet Assigned Numbers Authority).

Les numéros de port sont comparables aux numéros de boîte postale. Une lettre peut comporter un code postal, une ville et une boîte postale. Le code postal et la ville permettent de diriger la lettre vers le service de tri postal approprié, tandis que la boîte postale garantit la livraison de la lettre à la personne à qui elle est adressée. De même, l'adresse IP sert à envoyer le paquet au bon serveur, tandis que le numéro de port TCP ou UDP garantit la transmission du paquet à l'application appropriée.

10.2 Vue d'ensemble des ports de la couche transport

10.2.2 Ports de services

Un numéro de port doit être associé aux services exécutés sur les hôtes pour que la communication soit possible. Un hôte distant qui tente de se connecter à un service attend de ce dernier qu'il utilise des ports et des protocoles de couche transport. Certains ports, définis dans la spécification RFC 1700, sont des ports bien connus et réservés à TCP et à UDP. 1

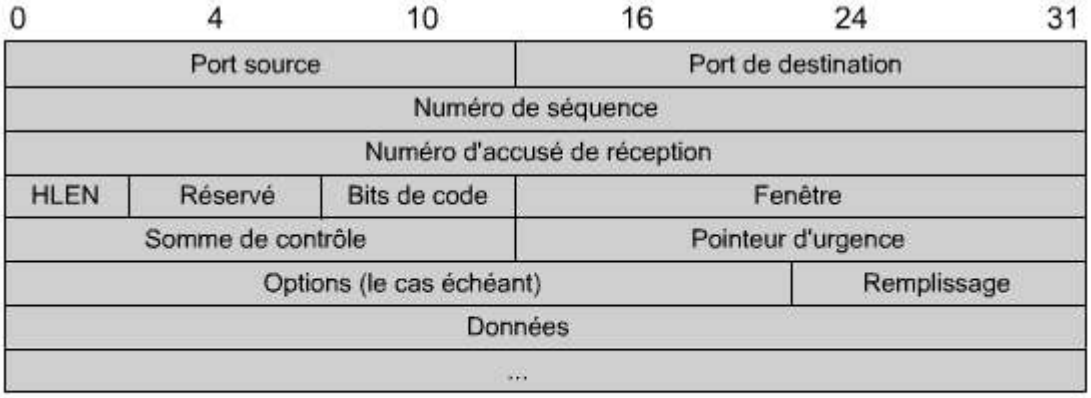
Décimal	Mot-clé	Description
0		Réservé
1-4		Non attribué
5	RJE	Soumission de travaux à distance
7	ECHO	Écho
9	DISCARD	Élimination
11	USERS	Utilisateurs actifs
13	DAYTIME	Heure du jour
15	NETSTAT	Who is Up ou NETSTAT
17	QUOTE	Citation du jour
19	CHARGEN	Générateur de caractères
20	FTP-DATA	Protocole FTP (données)
21	FTP	Protocole FTP
23	TELNET	Connexion en mode terminal
25	SMTP	Protocole SMTP (Simple Mail Transfer Protocol)
37	TIME	Heure du jour
39	RLP	Protocole RLP (Resource Location Protocol)
42	NAMESERVER	Serveur de noms d'hôte
43	NICNAME	Who Is
53	DOMAIN	Serveur de noms de domaine
67	BOOTPS	Serveur de protocole Bootstrap
68	BOOTPC	Client de protocole Bootstrap
69	TFTP	Protocole TFTP (Trivial File Transfer Protocol)
75		Tout service de sortie privé
77		Any Private RJE Service
79	FINGER	Finger
80	HTTP	Protocole HTTP
95	SUPDUP	Protocole SUPDUP
101	HOSTNAME	Serveur de noms d'hôte NIC
102	ISO-TSAP	ISO-TSAP
110	POP3	Protocole POP (Post Office Protocol) permettant au client de récupérer des messages à partir d'un serveur de messagerie
113	AUTH	Service d'authentification
117	UUCP-PATH	Service de chemin UUCP
123	NTP	Protocole NTP (Network Time Protocol)
133-159		Non attribué
160-223		Réservé
224-241		Non attribué
242-255		Non attribué

Ces ports bien connus définissent les applications exécutées au niveau supérieur des protocoles de couche transport. Par exemple, un serveur exécutant le service FTP transmet des connexions TCP via les ports 20 et 21 entre des clients et son application FTP. Ainsi, le serveur peut déterminer avec exactitude le service demandé par un client. Les protocoles TCP et UDP utilisent des numéros de port pour déterminer le service auquel les requêtes sont destinées.

10.2 Vue d'ensemble des ports de la couche transport

10.2.3 Ports de clients

Chaque fois qu'un client se connecte à un service sur un serveur, un port source et un port de destination doivent être spécifiés. Les segments TCP et UDP contiennent des champs pour les ports source et de destination. 1 2 Les ports de destination, ou ports de services, sont normalement définis à l'aide des ports bien connus. Les ports source définis par le client sont déterminés de manière dynamique.



Voici la structure des champs d'un segment TCP, composé d'un en-tête TCP suivi de données. Les segments servent à établir les connexions, ainsi qu'à transporter les données et les accusés de réception.

Nombre de bits	16	16	16	16	16
	Port source	Port de destination	Longueur	Somme de contrôle	Données...

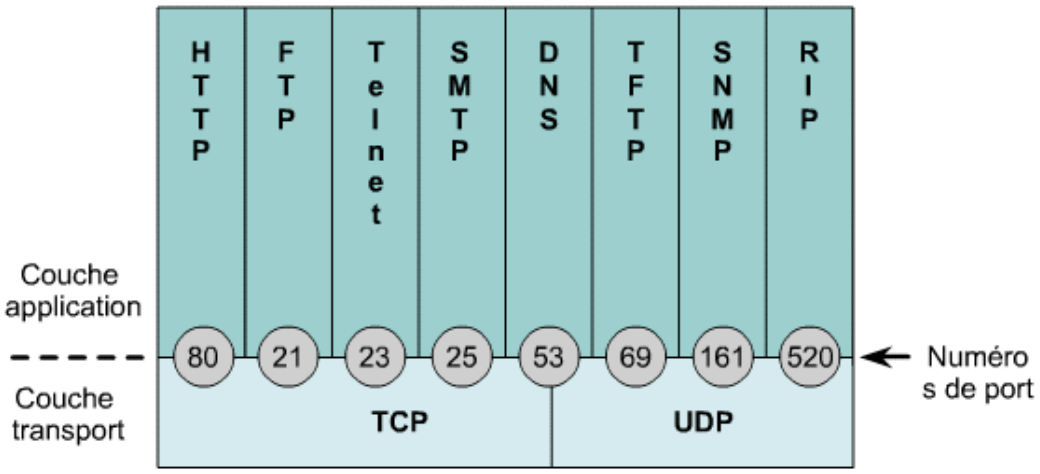
Aucun champ de séquence ou d'accusé de réception.

En règle générale, un client détermine le port source en affectant de manière aléatoire un numéro supérieur à 1023. Par exemple, un client qui tente de communiquer avec un serveur Web utilise TCP et règle le port de destination sur 80 et le port source sur 1045. Lorsque le paquet arrive sur le serveur, il est transmis à la couche transport, puis au service HTTP qui est exécuté au niveau du port 80. Le serveur HTTP répond à la requête du client avec un segment qui utilise le port 80 comme source et le port 1045 comme destination. De cette manière, les clients et les serveurs utilisent des ports pour distinguer le processus auquel le segment est associé.

10.2 Vue d'ensemble des ports de la couche transport

10.2.4 Numérotation des ports et numéros de port bien connus

Les numéros de port sont représentés par 2 octets dans l'en-tête d'un segment TCP ou UDP. Cette valeur sur 16 bits peut représenter des numéros de port compris entre 0 et 65535, qui sont répartis en trois catégories: les ports bien connus, les ports enregistrés, et les ports dynamiques ou privés. Les 1023 premiers ports sont des ports bien connus. Comme leur nom l'indique, ces ports sont utilisés pour des services de réseaux bien connus, tels que FTP, Telnet ou DNS. 1 Les ports enregistrés sont compris entre 1024 et 49151. Les ports compris entre 49152 et 65535 sont des ports dits dynamiques ou privés.



Activité de média interactive

Glisser-Positionner : Numéros de port

À la fin de cette activité, l'étudiant sera en mesure de comprendre les numéros de port.

10.2 Vue d'ensemble des ports de la couche transport
10.2.5 Exemple de sessions multiples entre des hôtes

Les numéros de port sont utilisés pour suivre des sessions multiples entre des hôtes. Les numéros de port source et de destination combinés à l'adresse réseau forment un socket. Un ensemble de deux sockets, un pour chaque hôte, forme une connexion unique. Par exemple, un hôte peut établir une connexion telnet sur le port 23 tout en surfant sur Internet via le port 80. Les adresses IP et MAC sont identiques car les paquets proviennent du même hôte. Par conséquent, chaque conversation côté source a besoin de son propre numéro de port, de même que chaque service demandé.

Numéros de port et socket

- Les numéros de port sont utilisés pour suivre des sessions multiples entre des hôtes.
- Un numéro de port combiné à l'adresse réseau forme un socket.

Activité de TP

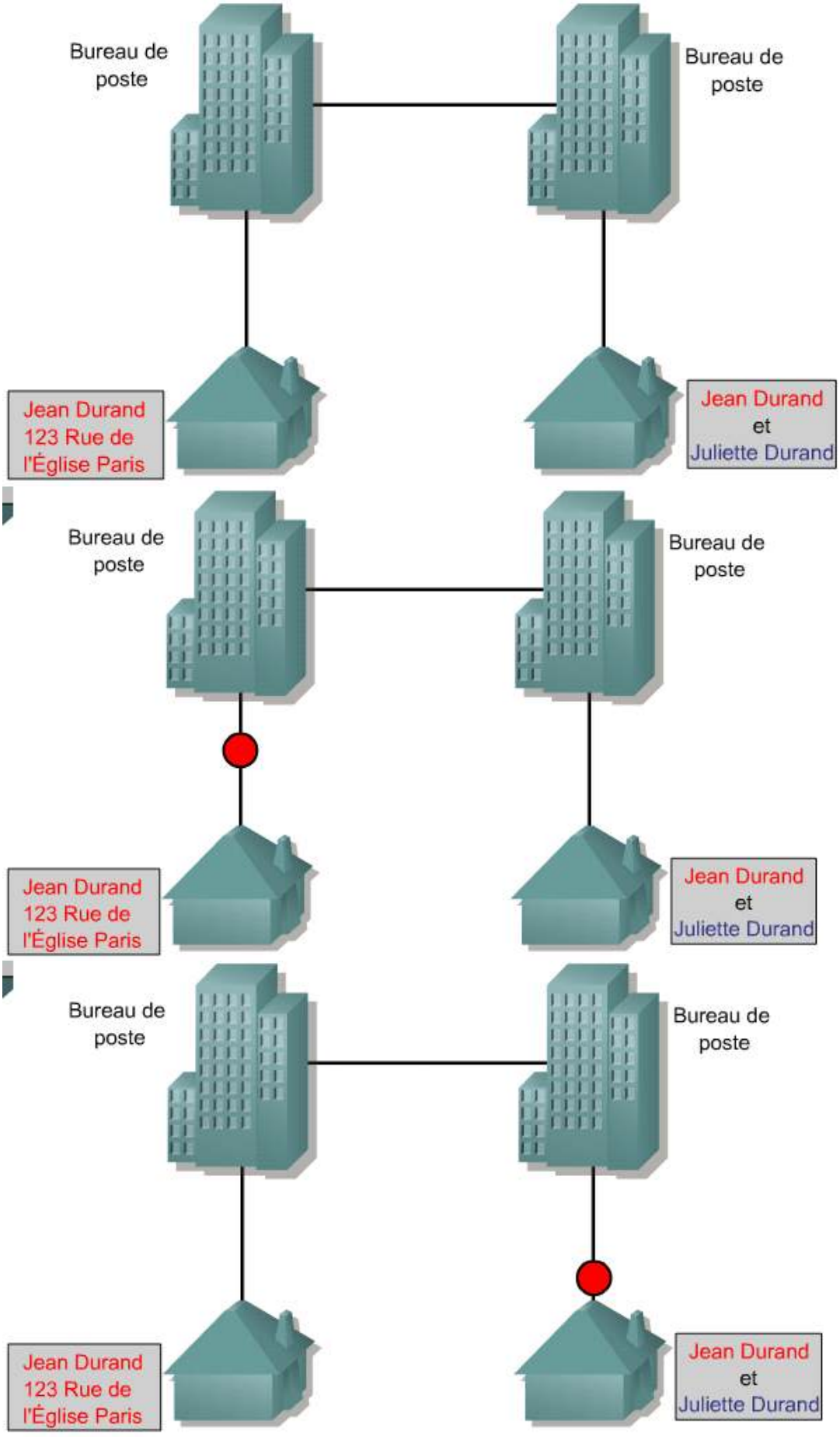
Exercice : Numéros de ports bien connus et sessions multiples

Au cours de ce TP, l'étudiant va activer des services HTTP sur un routeur.

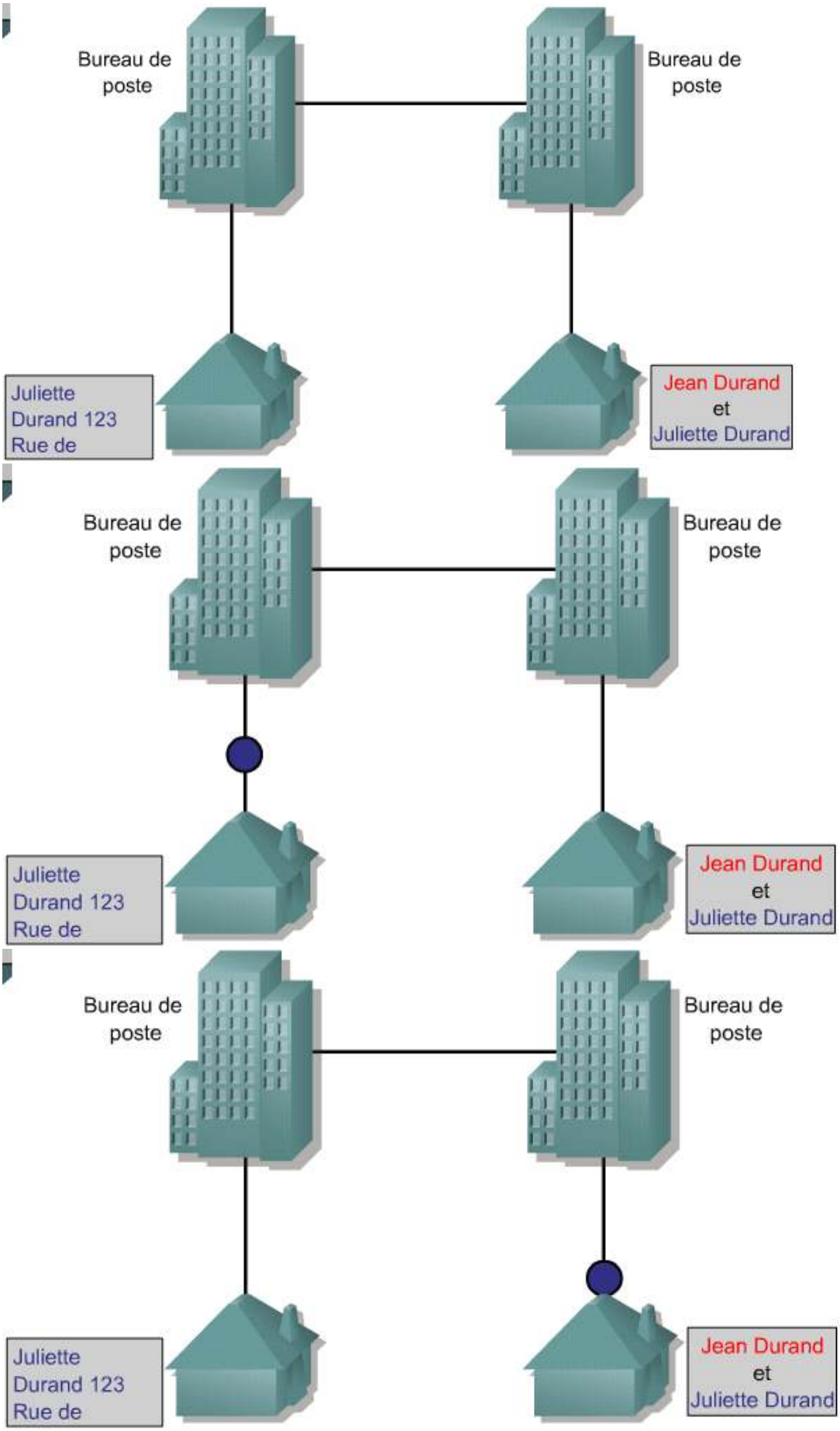
10.2 Vue d'ensemble des ports de la couche transport
10.2.6 Comparaison des adresses MAC, des adresses IP et des numéros de port

Ces trois méthodes d'adressage sont souvent confondues, mais cette confusion peut être évitée si les adresses sont expliquées par rapport au modèle OSI. Les numéros de port sont situés au niveau de la couche transport et sont desservis par la couche réseau. La couche réseau affecte l'adresse logique (adresse IP) et est ensuite desservie par la couche liaison de données qui affecte l'adresse physique (adresse MAC).

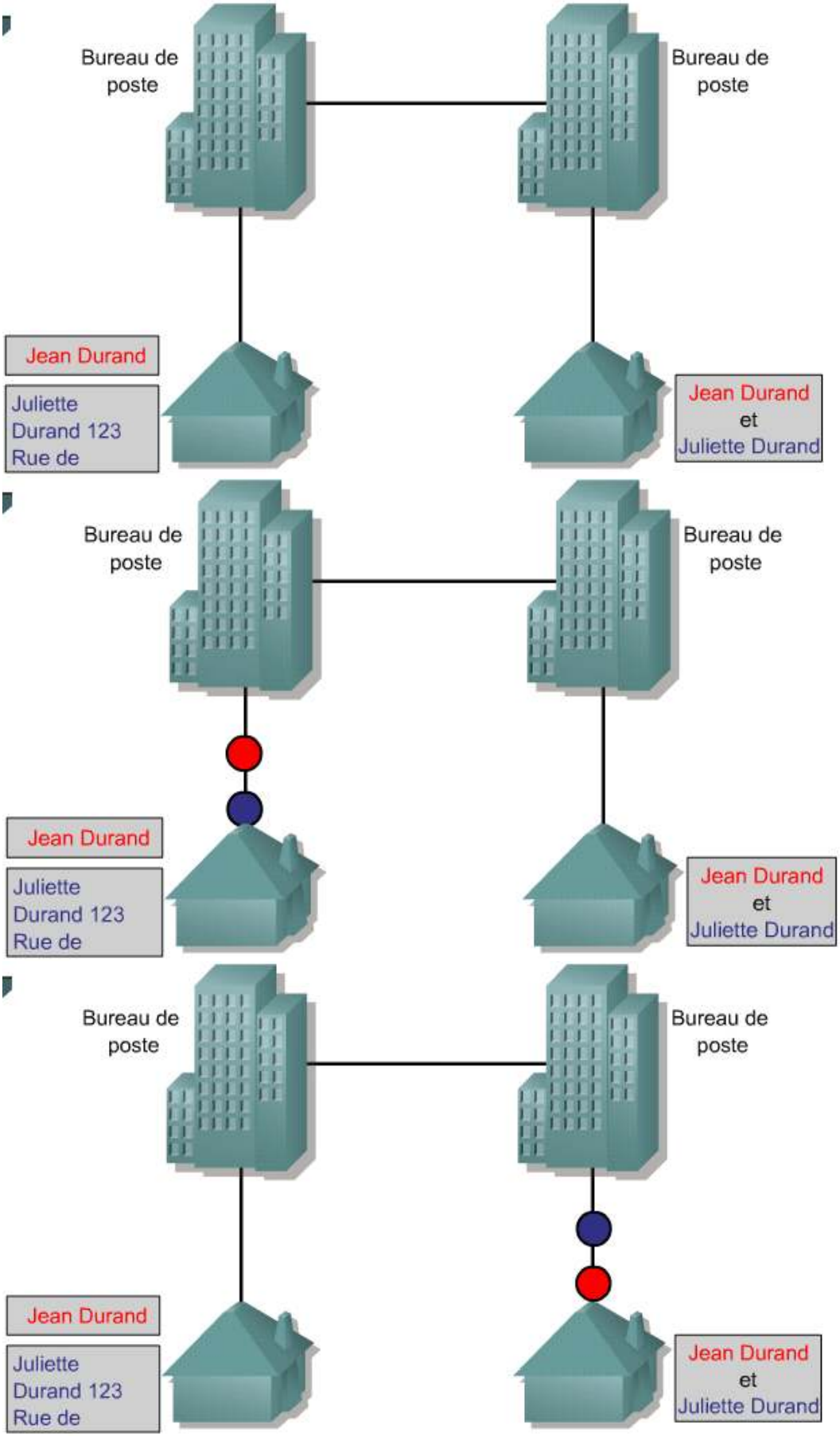
Le processus s'apparente à l'envoi d'une lettre normale. Sur une lettre, l'adresse est composée d'un nom, de la rue et de la ville. Ces éléments sont comparables au numéro de port, à l'adresse MAC et à l'adresse IP utilisés pour les données de réseau. Le nom sur l'enveloppe équivaut au numéro de port, le numéro civique ainsi que le nom de la rue correspondent à l'adresse MAC et la ville représente l'adresse IP. Plusieurs lettres peuvent être envoyées à la même adresse, mais contenir des noms différents. Par exemple, deux lettres peuvent être envoyées à la même destination, mais l'une peut être adressée à Jean Durand et l'autre à Juliette Durand. Cela est comparable aux sessions multiples avec des numéros de port différents. [1]


Bureau de poste
Bureau de poste
Jean Durand 123 Rue de l'Église Paris
Jean Durand et Juliette Durand
Bureau de poste
Bureau de poste
Jean Durand 123 Rue de l'Église Paris
Jean Durand et Juliette Durand
Bureau de poste
Bureau de poste
Jean Durand 123 Rue de l'Église Paris
Jean Durand et Juliette Durand

2


Bureau de poste
Bureau de poste
Juliette Durand 123 Rue de
Jean Durand et Juliette Durand
Bureau de poste
Bureau de poste
Juliette Durand 123 Rue de
Jean Durand et Juliette Durand
Bureau de poste
Bureau de poste
Juliette Durand 123 Rue de
Jean Durand et Juliette Durand

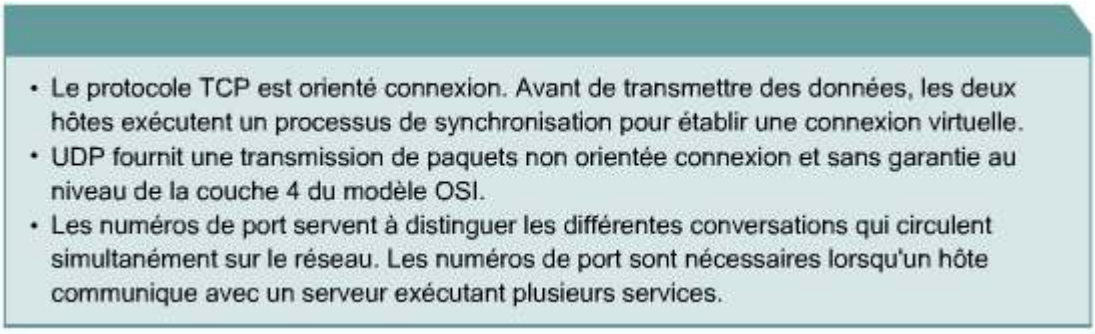
3


Bureau de poste
Bureau de poste
Jean Durand
Juliette Durand 123 Rue de
Jean Durand et Juliette Durand
Bureau de poste
Bureau de poste
Jean Durand
Juliette Durand 123 Rue de
Jean Durand et Juliette Durand
Bureau de poste
Bureau de poste
Jean Durand
Juliette Durand 123 Rue de
Jean Durand et Juliette Durand

Résumé

La compréhension des points clés suivants devrait être acquise:

- Description du fonctionnement du protocole TCP
- Processus de synchronisation (échange en trois étapes)
- Attaques par déni de service
- Fenêtrage et taille de fenêtre
- Numéros de séquence
- Accusé de réception positif
- Fonctionnement du protocole UDP
- Conversations multiples entre hôtes
- Ports de services
- Ports de clients
- Numérotation des ports et numéros de port bien connus
- Exemple de sessions multiples entre des hôtes
- Comparaison des adresses MAC, des adresses IP et des numéros de port



Vue d'ensemble

Les administrateurs réseau doivent trouver le moyen d'interdire l'accès au réseau à certains utilisateurs tout en permettant aux utilisateurs internes d'accéder aux services nécessaires. Bien que les outils permettant d'assurer la sécurité, tels que les mots de passe, l'équipement de rappel et les dispositifs de sécurité physiques, se révèlent utiles, dans la plupart des cas, ils n'offrent pas la souplesse que procurent le filtrage de trafic de base et les contrôles spécifiques que leur préfèrent la majorité des administrateurs. Ainsi, il se peut qu'un administrateur réseau souhaite accorder l'accès à Internet aux utilisateurs, tout en interdisant à des utilisateurs externes l'accès au réseau LAN via Telnet.

Les routeurs assurent les fonctions de base de filtrage du trafic, telles que le blocage du trafic Internet, à l'aide de listes de contrôle d'accès. Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus qui s'appliquent aux adresses ou aux protocoles de couche supérieure. Ce module présente les listes de contrôle d'accès standard et étendues permettant de contrôler le trafic réseau, ainsi que le rôle de ces listes dans le cadre d'une solution de sécurité.

En outre, ce module comprend des conseils, des éléments dont il faut tenir compte, des recommandations et des lignes directrices générales sur l'utilisation des listes de contrôle d'accès, en plus des commandes et des configurations nécessaires à la création de ces listes. Enfin, ce chapitre présente des exemples de listes de contrôle d'accès standard et étendues, ainsi que des méthodes d'application de ces listes aux interfaces de routeur.

Les listes de contrôle d'accès peuvent se limiter à une simple ligne destinée à autoriser des paquets à partir d'un hôte spécifique ou peuvent être constituées d'ensembles de règles et de conditions extrêmement complexes pouvant définir avec précision le trafic et les performances des processus de routeur. Tandis que la plupart des utilisations avancées des listes de contrôle d'accès sortent du cadre de ce cours, ce module fournit des détails sur les listes de contrôle d'accès standard et étendues, sur leur emplacement exact et sur certaines applications spéciales de ces listes.

À la fin de ce module, les étudiants doivent être en mesure de:

- Expliquer les différences entre les ACL standard et étendues
- Expliquer les règles de placement des ACL
- Créer et appliquer des ACL nommées
- Décrire la fonction de pare-feu

- Utiliser les ACL pour limiter l'accès au terminal virtuel

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
11.1	Notions de base sur la liste de contrôle d'accès (ACL)
11.2	Listes de contrôle d'accès (ACL)

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Développement d'une liste de contrôle d'accès répondant aux spécifications des utilisateurs	• Mise en œuvre de listes de contrôle d'accès	• Dépannage d'une liste de contrôle d'accès	

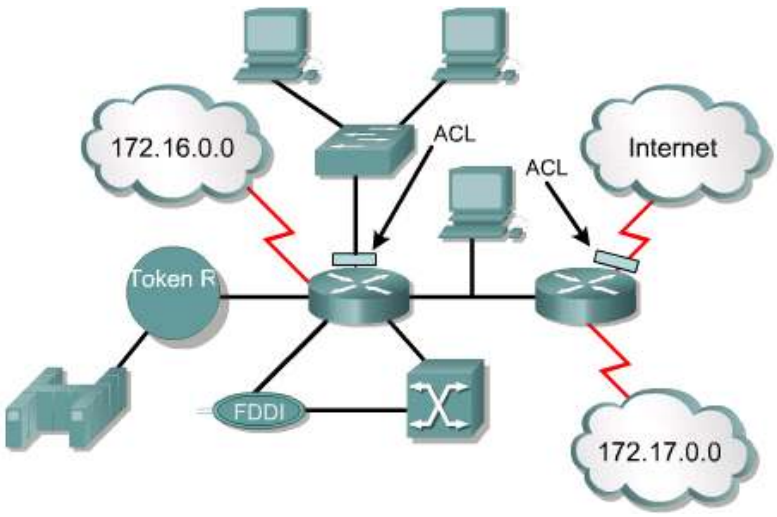
Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et	Dépannage	Technologie
• Développement d'une liste de contrôle d'accès répondant aux spécifications des utilisateurs	• Mise en œuvre de listes de contrôle d'accès	• Dépannage d'une liste de contrôle d'accès	

11.1 Notions de base sur la liste de contrôle d'accès (ACL)

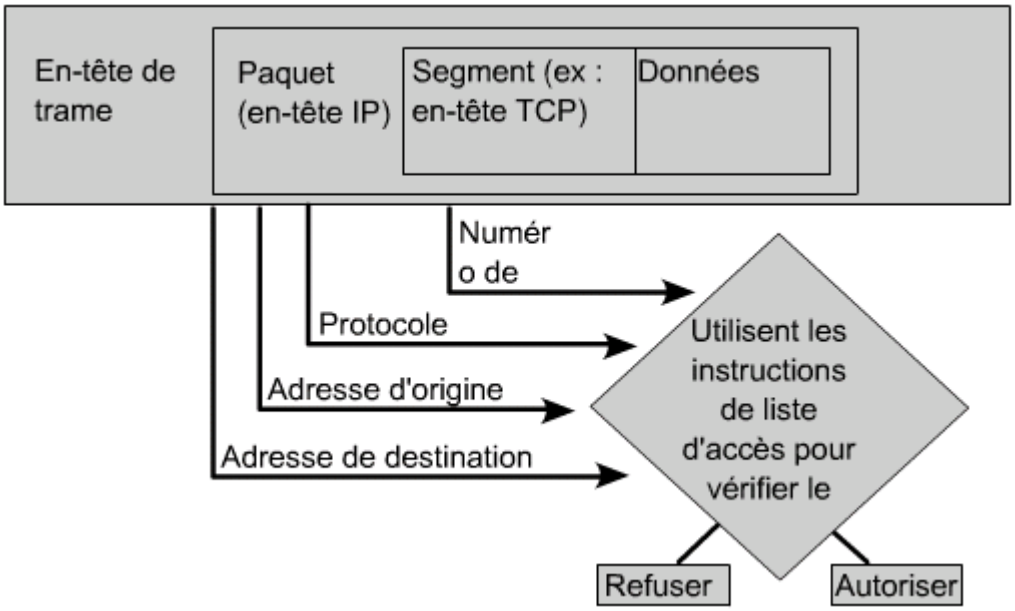
11.1.1 Définition des listes de contrôle d'accès

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées au trafic circulant via une interface de routeur. 1 Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter. L'acceptation et le refus peuvent être basés sur des conditions précises. Les ACL permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie.



Des listes de contrôle d'accès peuvent être créées pour tous les protocoles routés, tels que les protocoles IP (Internet Protocol) et IPX (Internetwork Packet Exchange). Des listes de contrôle d'accès peuvent également être configurées au niveau du routeur en vue de contrôler l'accès à un réseau ou à un sous-réseau.

Les listes d'accès filtrent le trafic réseau en commandant aux interfaces d'un routeur d'acheminer ou de bloquer des paquets routés. 2 Le routeur examine chaque paquet afin de déterminer s'il doit l'acheminer ou le rejeter en fonction des conditions précisées dans la liste de contrôle d'accès. Certaines conditions dans une ACL sont des adresses source et de destination, des protocoles et des numéros de port de couche supérieure.



Les listes de contrôle d'accès doivent être définies en fonction d'un protocole, d'une direction ou d'une interface. 3

Une liste par interface, par direction, par protocole

Avec deux interfaces et trois protocoles, ce routeur peut avoir un total de 12 ACL distinctes d'appliquées.

Pour contrôler le flux du trafic sur une interface, une ACL doit être définie pour chaque protocole activé sur l'interface. Les ACL contrôlent le trafic dans une seule direction à la fois sur une interface. Une ACL séparée doit être créée pour chaque direction : une pour le trafic entrant et une pour le trafic sortant. Enfin, chaque interface peut avoir plusieurs protocoles et directions définis. Si le routeur a deux interfaces configurées pour IP, AppleTalk et IPX, 12 listes d'accès distinctes sont nécessaires : une liste pour chaque protocole, fois deux pour la direction (entrée et sortie), fois deux pour le nombre d'interfaces.

Voici les principales raisons pour lesquelles il est nécessaire de créer des listes de contrôle d'accès :

- Limiter le trafic réseau et accroître les performances. En limitant le trafic vidéo, par exemple, les listes de contrôle d'accès permettent de réduire considérablement la charge réseau et donc d'augmenter les performances.
- Contrôler le flux de trafic. Les ACL peuvent limiter l'arrivée des mises à jour de routage. Si aucune mise à jour n'est requise en raison des conditions du réseau, la bande passante est préservée.
- Fournir un niveau de sécurité d'accès réseau de base. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section. Par exemple, l'hôte A peut accéder au réseau réservé aux ressources humaines, tandis que l'hôte B ne peut pas y accéder.
- Déterminer le type de trafic qui sera acheminé ou bloqué au niveau des interfaces de routeur. Il est possible d'autoriser l'acheminement des messages électroniques et de bloquer tout le trafic via Telnet.
- Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.

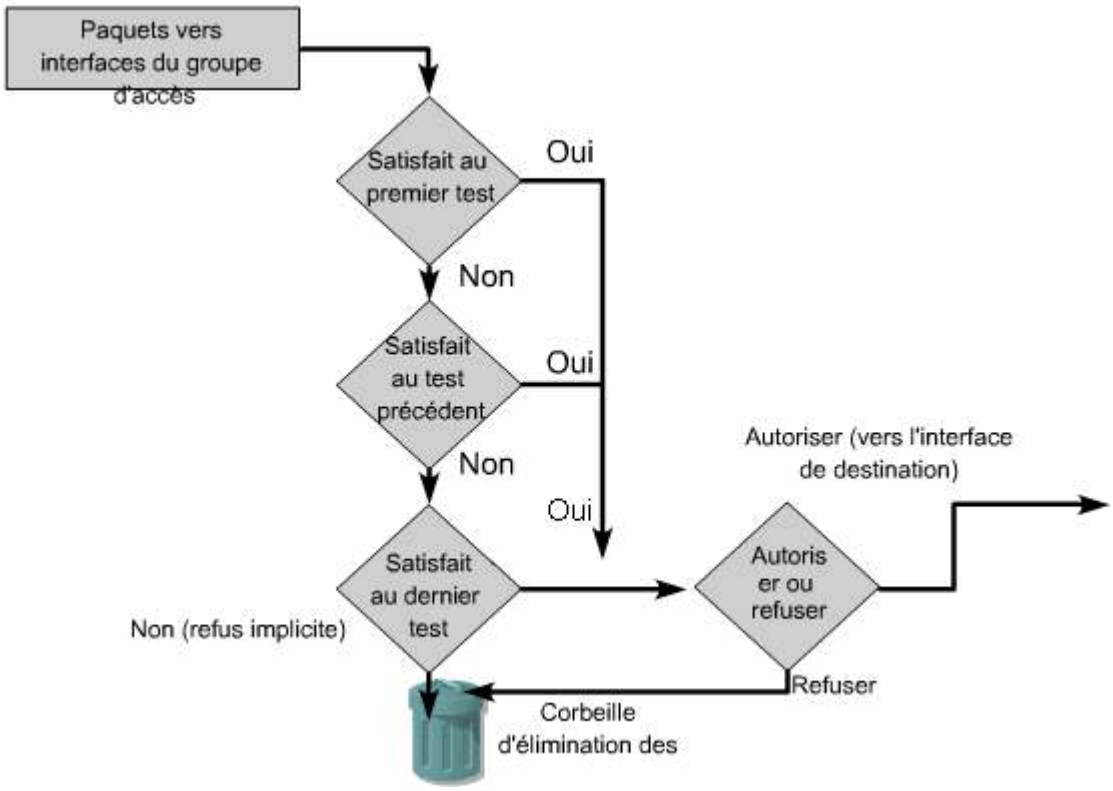
- Filtrer certains hôtes afin de leur accorder ou de leur refuser l'accès à une section de réseau. Accorder ou refuser aux utilisateurs la permission d'accéder à certains types de fichiers, tels que FTP ou HTTP.

Lorsqu'aucune liste de contrôle d'accès n'est configurée sur le routeur, tous les paquets acheminés par le routeur peuvent accéder à toutes les sections du réseau.

11.1 Notions de base sur la liste de contrôle d'accès (ACL)

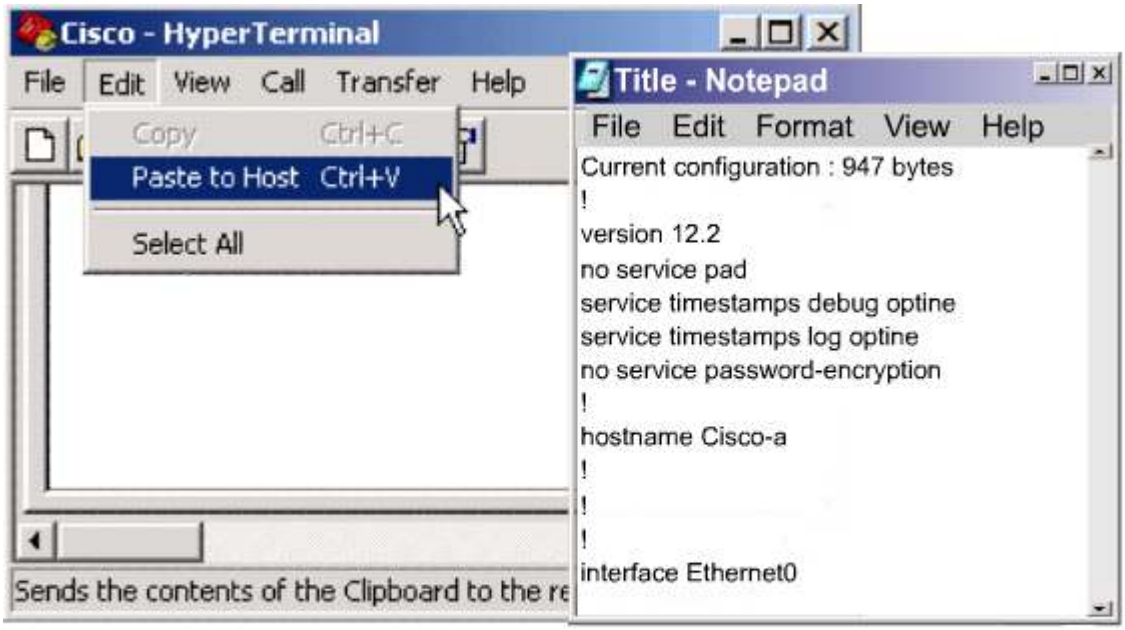
11.1.2 Fonctionnement des listes de contrôle d'accès

Une liste de contrôle d'accès est un groupe d'instructions qui définissent si les paquets sont acceptés ou rejetés au niveau des interfaces d'entrée et de sortie. 1Pour prendre ces décisions, les paquets sont comparés avec une instruction de condition d'une liste d'accès, puis acceptés ou rejetés selon l'action définie dans l'instruction.



L'ordre des instructions ACL est important. La plate-forme logicielle Cisco IOS teste le paquet par rapport à chaque instruction de condition en partant du début de la liste jusqu'à la fin. Lorsqu'une condition est satisfaite dans la liste, le paquet est accepté ou rejeté et les autres instructions ne sont pas vérifiées. Si une instruction de condition autorisant l'accès à tout le trafic est située en haut de la liste, aucune instruction ajoutée en dessous ne sera vérifiée.

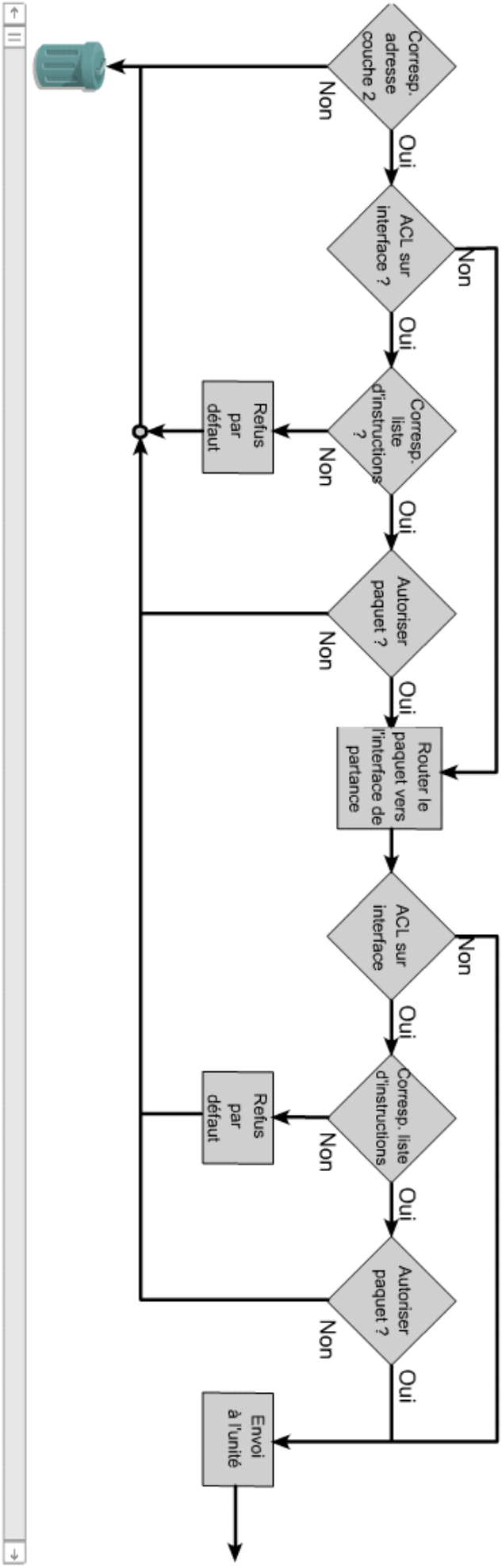
Pour ajouter des instructions de condition supplémentaires dans une liste d'accès, vous devez supprimer toute la liste et en recréer une avec les nouvelles instructions. 2Pour faciliter le processus de révision d'une liste de contrôle d'accès, il est préférable d'utiliser un éditeur de texte comme le Bloc-notes et de coller la liste dans la configuration du routeur.



Prenez l'habitude de mettre à jour les fichiers de configuration de votre routeur avec un éditeur de texte. Utilisez ensuite la fonction de collage vers hôte dans HyperTerminal pour insérer la mise à jour dans le routeur.

Le processus du routeur débute de la même façon, et ce, que des listes de contrôle d'accès soient utilisées ou non. 3 Au moment où une trame entre dans l'interface, le routeur vérifie si l'adresse de couche 2 correspond ou s'il s'agit d'une trame de broadcast. Si l'adresse de la trame est acceptée, les informations de trame sont éliminées et le routeur recherche une liste de contrôle d'accès sur l'interface d'entrée. Le cas échéant, le paquet est vérifié pour déceler des correspondances avec les instructions de la liste. Si le paquet correspond à une instruction, il est soit accepté soit refusé. Si le paquet est accepté dans l'interface, il est ensuite comparé aux enregistrements de la table de routage afin de déterminer l'interface de destination, et transmis à cette interface. Ensuite, le routeur vérifie si l'interface de destination possède une liste de contrôle d'accès. Le cas échéant, le paquet est à présent comparé aux instructions de cette liste et si une correspondance est trouvée, il est soit accepté soit rejeté. En l'absence de liste de contrôle d'accès ou si le paquet est accepté, il est encapsulé dans le nouveau protocole de couche 2 et acheminé par l'interface jusqu'à l'unité suivante.

En résumé, les instructions d'une liste de contrôle d'accès fonctionnent dans l'ordre séquentiel logique. Si une condition est satisfaite, le paquet est autorisé ou refusé et les autres instructions ne sont pas vérifiées. Si aucune des instructions ne correspond au paquet, une instruction implicite **`deny any`** est placée à la fin de la liste par défaut. L'instruction invisible **`deny any`** sur la dernière ligne d'une ACL interdit l'accès de tout paquet qui ne correspond pas aux instructions de la liste de contrôle d'accès. Lorsque vous créez une ACL pour la première fois, il est recommandé d'ajouter l'instruction **`deny`** à la fin de la liste pour renforcer la présence dynamique de l'interdiction implicite.


Corresp. adresse couche 2
Non
Oui
ACL sur interface ?
Non
Oui
Corresp. liste d'instructions ?
Refus par défaut
Non
Oui
Autoriser paquet ?
Non
Oui
Router le paquet vers l'interface de partance
ACL sur interface
Non
Oui
Corresp. liste d'instructions
Refus par défaut
Non
Oui
Autoriser paquet ?
Non
Oui
Envoi à l'unité

```
Router(config)#
```

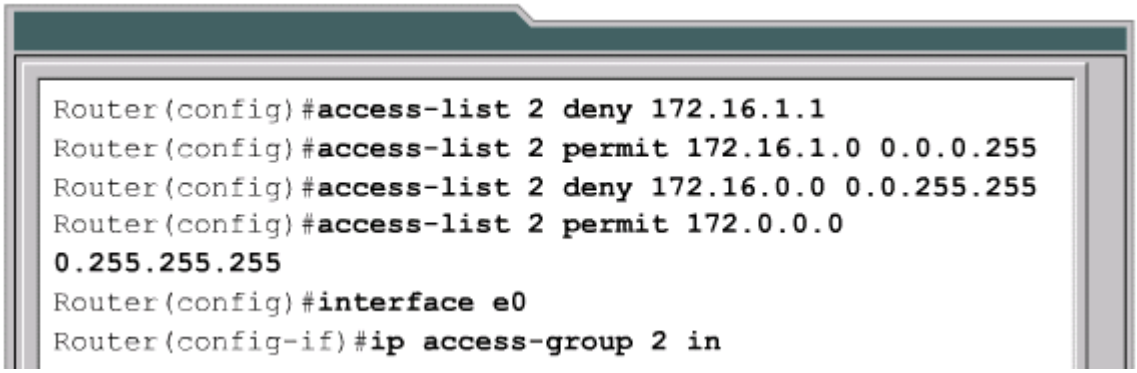
Les ACL sont créées en mode de configuration globale. 1 Il existe différents types de listes de contrôle d'accès : standard, étendues, IPX et AppleTalk. Au moment de configurer les listes de contrôle d'accès d'un routeur, vous devez identifier chaque liste en lui attribuant un numéro unique. Ce numéro identifie le type de liste d'accès créé et doit être compris dans la plage de numéros valide pour ce type. 2

Protocole	Plage
IP standard	1-99, 1300-1999
IP étendu	100-199, 2000-2699
AppleTalk	600-699
IPX	800-899
IPX étendu	900-999
Protocole IPX Service Advertising	1000-1099

Après avoir accédé au mode de commande approprié et décidé d'un numéro de type de liste, l'utilisateur saisit les instructions de la liste d'accès à l'aide de la commande **access-list**, suivi des paramètres appropriés. 3 La seconde partie du processus consiste à les assigner à l'interface qui convient. Cette première étape est la première d'un processus qui en compte deux. La seconde partie du processus consiste à assigner l'ACL à l'interface qui convient.

Étape 1	Définir la liste de contrôle d'accès à l'aide de la commande suivante : `Router(config)#access-list access-list-number (permit | deny) {test-conditions}` Un énoncé global identifie la liste de contrôle d'accès. Plus particulièrement, la plage 1 à 99 est réservée à l'accès IP standard. Ce numéro indique le type de liste de contrôle d'accès. Dans la plate-forme logicielle Cisco IOS version 11.2 ou ultérieure, les listes de contrôle d'accès peuvent aussi être identifiées par un nom, tel que groupe_formation, plutôt que par un numéro. Les termes " permit " et " deny " dans l'énoncé global de liste de contrôle d'accès indiquent comment les paquets qui satisfont aux conditions de test sont traités par la plate-forme logicielle Cisco IOS. " Permit " signifie généralement que le paquet pourra utiliser une ou plusieurs des interfaces que vous préciserez plus tard. Le ou les paramètres finaux précisent les conditions de test utilisées par l'énoncé de liste de contrôle d'accès.
Étape 2	Vous devez ensuite appliquer les listes de contrôle d'accès à une interface à l'aide de la commande access-group, comme dans cet exemple : `Router(config-if)#(protocol) access-group access-list-number` Tous les énoncés de liste de contrôle d'accès identifiés par numéro-liste-accès sont associés à une ou à plusieurs interfaces. Tout paquet qui satisfait aux conditions de test de la liste de contrôle d'accès est autorisé à utiliser une interface du groupe d'accès d'interfaces.

Sous TCP/IP, les listes de contrôle d'accès sont affectées à une ou à plusieurs interfaces et peuvent filtrer le trafic entrant ou sortant à l'aide de la commande **`ip access-group`** disponible à partir du mode de configuration d'interface. 4



Lorsque vous affectez une ACL à une interface, vous devez spécifier la direction du filtre (entrée ou sortie). La direction du filtre peut être définie de manière à vérifier les paquets qui sont reçus ou envoyés par une interface. Pour déterminer si une liste de contrôle d'accès concerne le trafic entrant ou sortant, l'administrateur réseau doit regarder les interfaces comme s'il était positionné à l'intérieur du routeur. Il s'agit d'un point très important. Les paquets reçus par une interface sont filtrés par une liste de contrôle d'accès pour trafic entrant tandis que les paquets envoyés par une interface sont filtrés par une liste de contrôle d'accès pour trafic sortant. Après avoir créé une liste d'accès numérotée, vous devez l'affecter à une interface. Une liste de contrôle d'accès contenant des instructions numérotées ne peut pas être modifiée. Elle doit être supprimée à l'aide des instructions de l'ACL en utilisant la commande **`no access-list`***`numéro-de-liste`* pour être ensuite recréée. 5

Les règles de base suivantes doivent être respectées lors de la création et de l'application des listes d'accès :

- Une liste d'accès par direction et par protocole.
- Les listes d'accès standard doivent être appliquées le plus près possible de la destination.
- Les listes d'accès étendues doivent être appliquées le plus près possible de la source.
- Pour faire référence à une interface d'entrée ou de sortie, placez-vous à l'intérieur du routeur en regardant l'interface en question.
- Les instructions sont traitées dans l'ordre depuis le début de la liste jusqu'à la fin jusqu'à ce qu'une correspondance soit trouvée. Si aucune correspondance n'est détectée, le paquet est refusé.
- Il existe un refus implicite **`deny any`** à la fin de toutes les listes de contrôle d'accès. Cela n'apparaît pas dans la liste de configuration.
- Les entrées de la liste d'accès doivent filtrer les paquets dans l'ordre, du plus spécifique au plus général. Les hôtes spécifiques doivent être rejetés en premier, tandis que les groupes ou les filtres généraux viennent en dernier.
- La condition de correspondance est examinée en premier. L'acceptation ou le refus est examiné UNIQUEMENT si la condition est vraie.
- Ne travaillez jamais avec une liste d'accès qui est appliquée de manière active.
- Utilisez un éditeur de texte pour créer des commentaires indiquant la logique, puis ajoutez les instructions correspondantes.
- Les nouvelles lignes sont toujours ajoutées à la fin de la liste de contrôle d'accès. La commande **`no access-list`***`x`* supprime toute la liste. Il n'est pas possible d'ajouter et de supprimer des lignes spécifiques dans des listes d'accès numérotées.
- Une liste d'accès IP envoie un message ICMP d'hôte inaccessible à l'émetteur du paquet rejeté et élimine le paquet dans la corbeille prévue à cet effet.
- Soyez particulièrement attentif lorsque vous supprimez une liste d'accès. Si la liste d'accès est appliquée à une interface de production et que vous la supprimez, selon la version de l'IOS, une instruction **`deny any`** peut être appliquée par défaut à l'interface et tout le trafic peut être arrêté.
- Les filtres de sortie ne concernent pas le trafic généré par le routeur local.

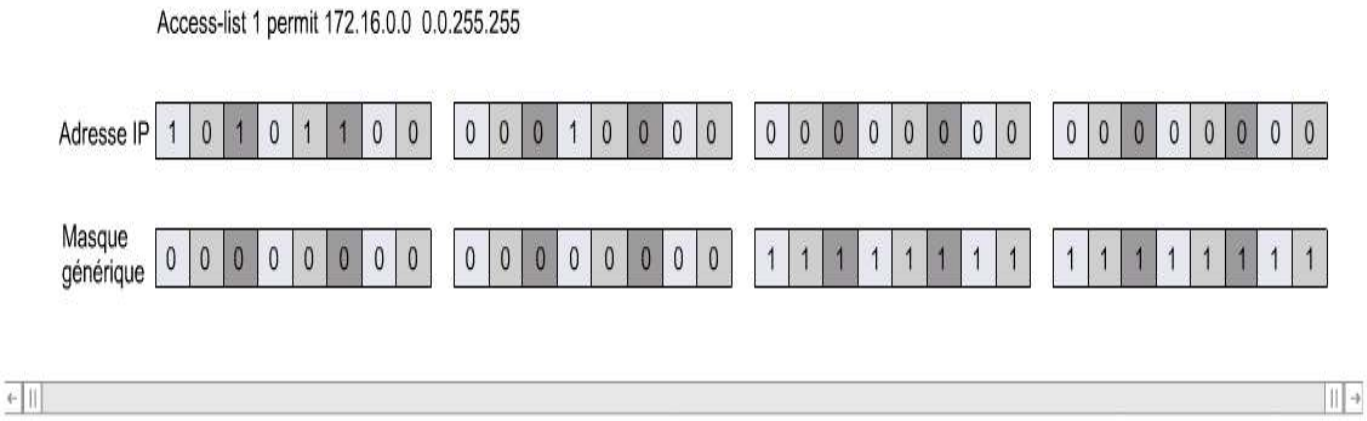
Activité de TP

Activité en ligne : Création de listes de contrôle d'accès

Au cours de ce TP, les étudiants vont explorer la syntaxe utilisée pour créer des listes de contrôle d'accès standard et étendues.

11.1 Notions de base sur la liste de contrôle d'accès (ACL)

11.1.4 Rôle du masque générique



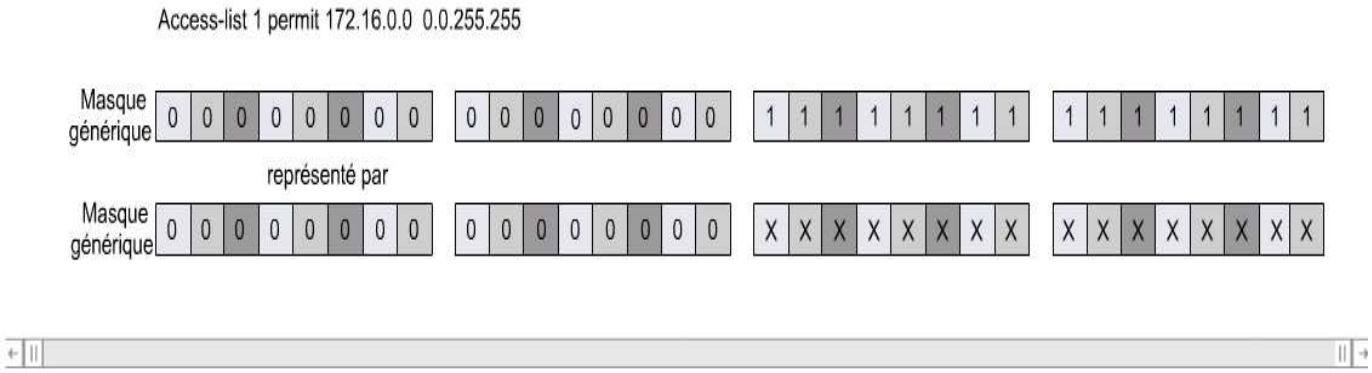
Ce masque générique permettra une concordance pour les adresses IP de 172.16.0.0 à 172.16.255.255. N'oubliez pas que la correspondance indique uniquement que cette instruction doit être appliquée au paquet. La liste de contrôle d'accès peut autoriser ou refuser l'accès au routeur.

Un masque générique est une quantité de 32 bits divisés en quatre octets. 1Un masque générique est jumelé à une adresse IP. Les chiffres 1 et 0 du masque sont utilisés pour indiquer la façon dont les bits de l'adresse IP correspondante doivent être traités. L'expression masque générique est un surnom du procédé de correspondance masque-bit des listes de contrôle d'accès. Les masques génériques n'ont aucune relation fonctionnelle avec les masques de sous-réseau. Ils sont utilisés dans des cas différents et suivent des règles différentes.

Le masque de sous-réseaux et le masque générique représentent deux choses différentes même s'ils sont tous les deux appliqués à des adresses IP. Les masques de sous-réseaux utilisent les uns et les zéros binaires pour identifier les parties réseau, sous-réseaux et hôte d'une adresse IP. Les masques génériques utilisent les uns et les zéros binaires pour filtrer des adresses IP individuelles ou de groupes pour autoriser ou refuser un accès à des ressources à l'aide d'une adresse IP précise. Le masque générique agit typiquement "à l'inverse" du masque sous-réseaux. Les seules ressemblances entre un masque générique et un masque de sous-réseaux sont leur taille de trente deux bits et leur usage de uns et de zéros binaires.

Cependant, dans un masque générique, la signification des uns et des zéros n'est pas la même que dans le masque de sous-réseau. 2Afin d'éliminer toute confusion dans les schémas, nous avons remplacé les chiffres 1 par des X dans les masques

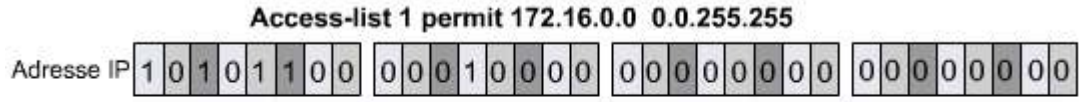
génériques. Le masque à la figure 2 serait écrit sous la forme 0.0.255.255.



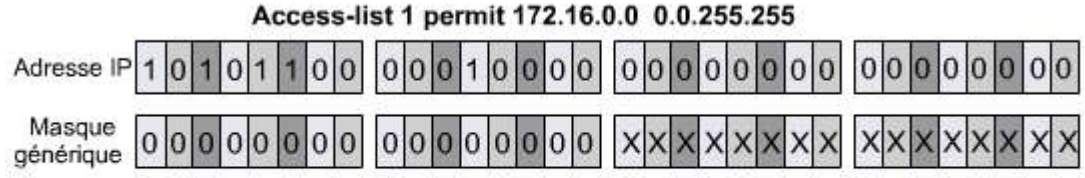
La substitution de X est utilisée pour réduire la confusion lorsque l'on applique le masque générique. C'est la convention qui sera d'ailleurs utilisée afin de démontrer l'utilisation des masques génériques dans le reste des illustrations de la section média.

Le zéro implique que la valeur soit comparée (correspondance parfaite exigée), tandis que le X (1) implique de bloquer la comparaison (correspondance exacte non exigée).

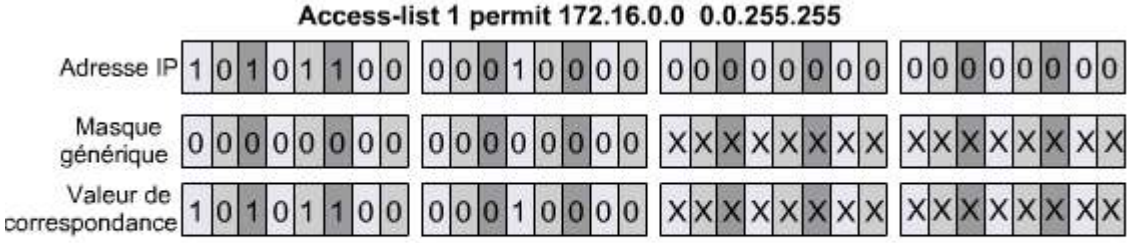
Dans le processus présenté, le masque générique est appliqué à l'adresse IP figurant dans l'instruction access-list. Cela crée la valeur de correspondance qui est utilisée pour voir si un paquet doit être traité par cette instruction ACL ou envoyé à l'instruction suivante pour être vérifié. Dans la deuxième partie du processus ACL, toute adresse IP vérifiée par une instruction ACL particulière se voit appliquer le masque générique correspondant à l'instruction. Le résultat de l'adresse IP et celui du masque générique doivent correspondre à la valeur de correspondance de l'ACL. À la figure 3, ce processus est illustré par une animation.



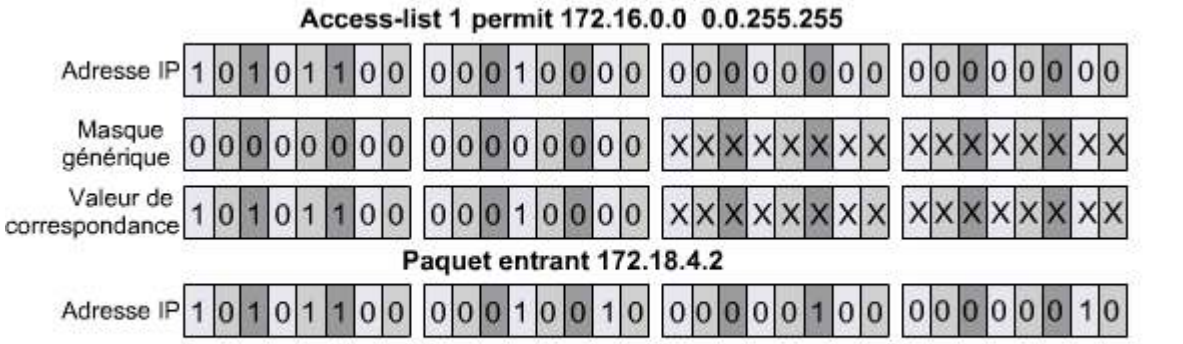
Afin d'utiliser cette instruction de liste d'accès, le routeur doit d'abord évaluer l'instruction ACL. Pour cela, il doit appliquer le masque générique à l'adresse IP indiquée dans l'instruction ACL.



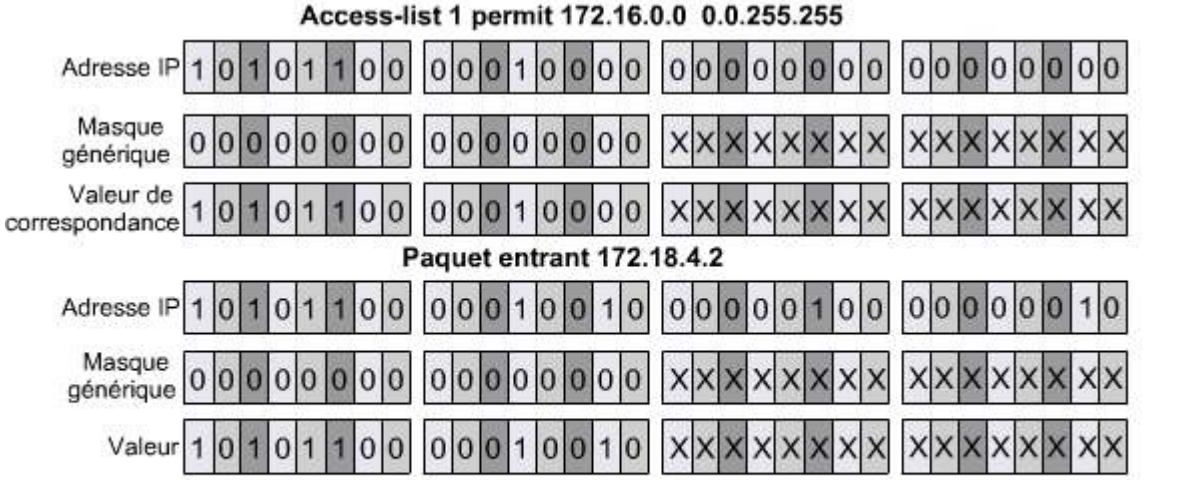
Le masque générique est appliqué à l'adresse IP. La valeur de correspondance est ainsi créée.



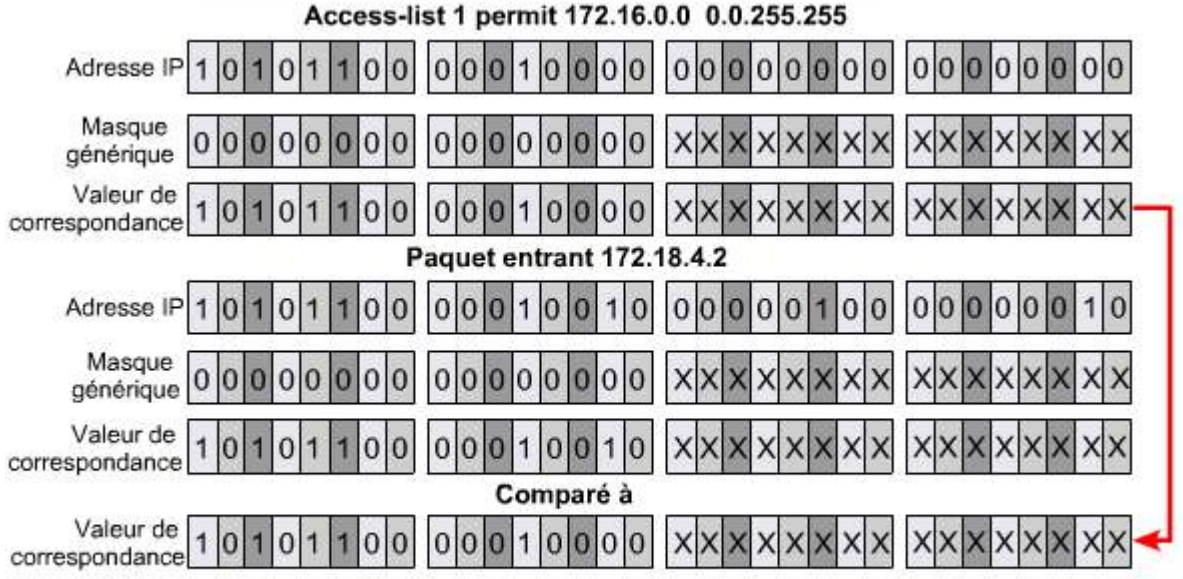
La valeur de correspondance est ce qui est réellement comparé à une adresse de paquet IP entrante ou sortante. Les étapes suivantes indiquent le processus.



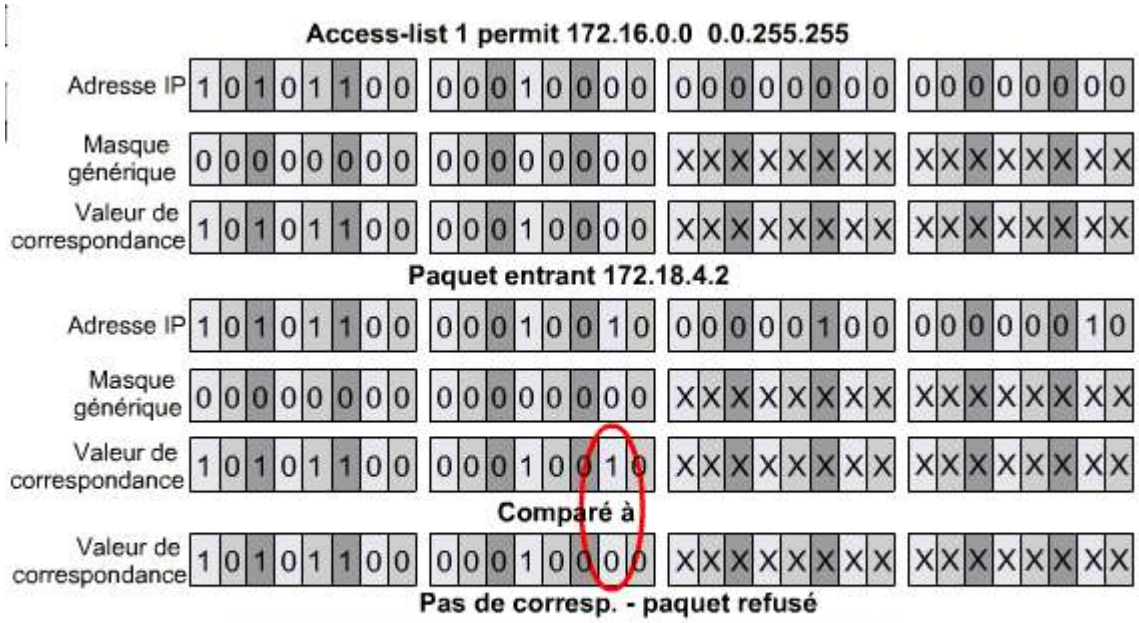
Le paquet IP 172.16.4.2 est reçu par l'interface et l'ACL lui est appliquée.



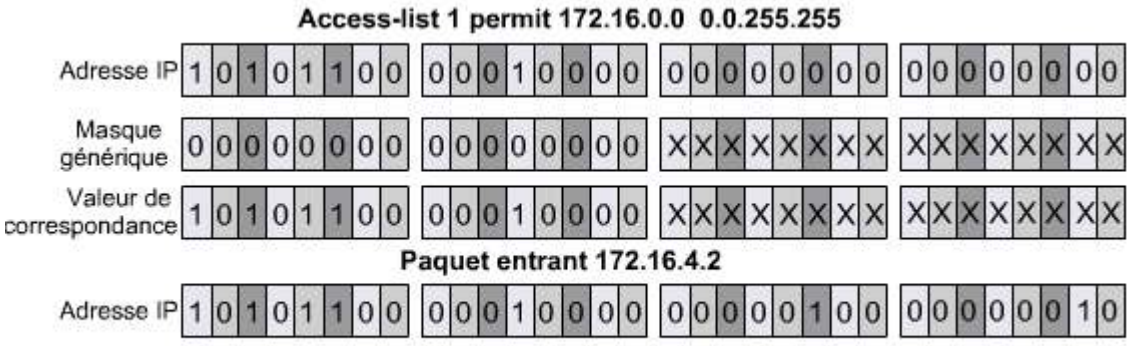
Le masque générique de l'instruction ACL est appliqué à l'adresse IP, ce qui génère la valeur à comparer à la valeur de correspondance.



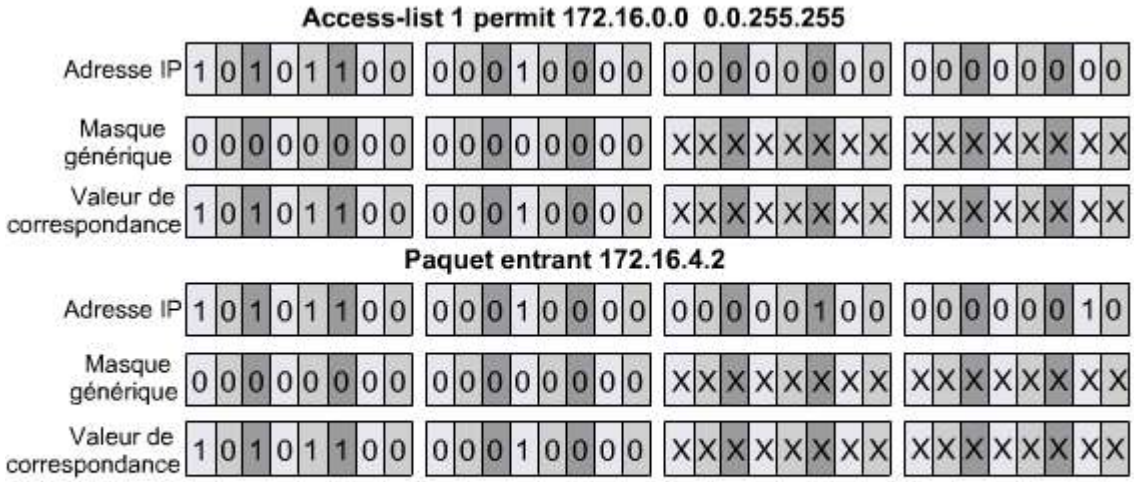
La valeur composée entrante est comparée à la valeur de correspondance interne.



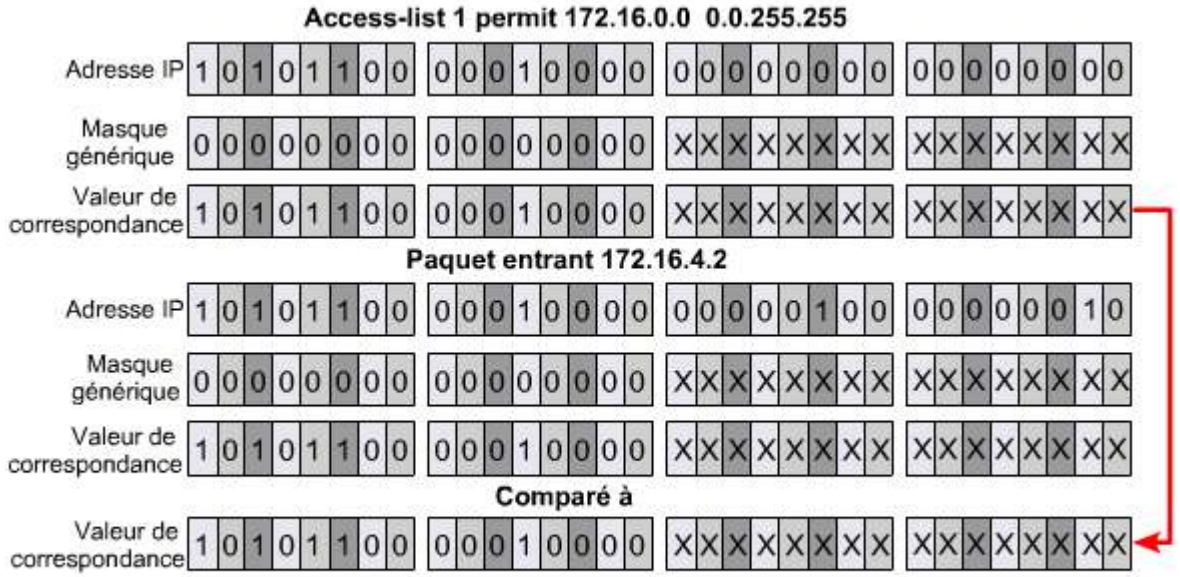
Dans le cas présent, les deux valeurs ne correspondent pas. Dans la comparaison, le deuxième bit du second octet est différent dans les deux valeurs de correspondance. Le paquet est donc refusé car il ne concorde pas.



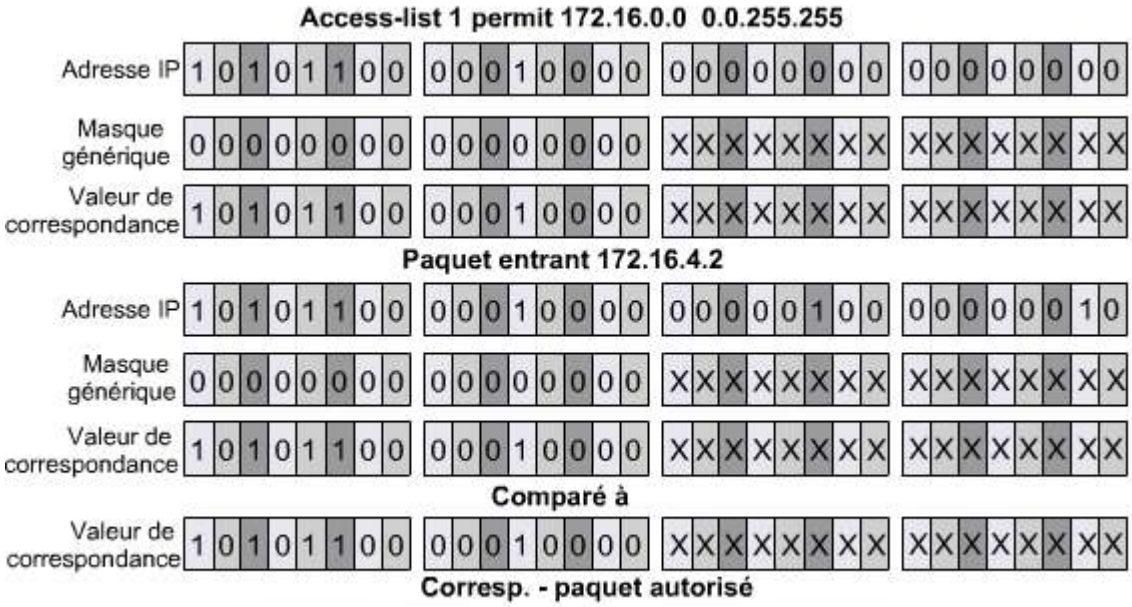
Un autre paquet est reçu par l'interface et l'ACL lui est appliquée.



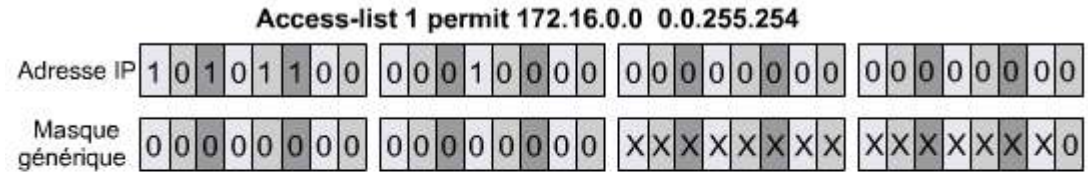
Le masque générique de l'instruction ACL est appliqué à cette adresse IP, ce qui génère la valeur à comparer à la valeur de correspondance.



La valeur composée entrante est comparée à la valeur de correspondance interne.

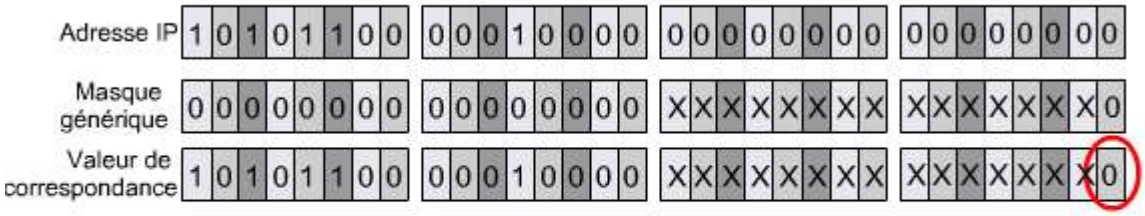


Dans le cas présent, les deux valeurs correspondent et le paquet est accepté.



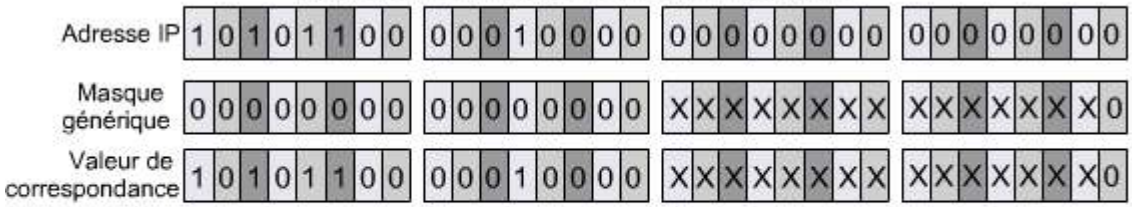
L'instruction ACL a maintenant changé pour autoriser tous les hôtes pairs compris entre 172.16.0.0 et 172.16.255.255. La seule modification par rapport à l'exemple précédent concerne le masque générique qui correspond maintenant à 0.0.255.254 au lieu de 0.0.255.255. La représentation binaire indique que le bit le plus à droite va être vérifié et qu'il doit être égal à zéro.

Access-list 1 permit 172.16.0.0 0.0.255.254

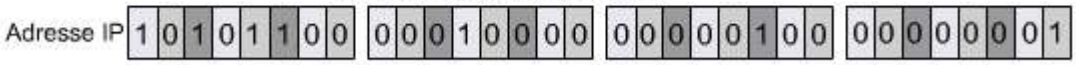


Notez que la valeur de correspondance comporte maintenant un zéro pour le bit le plus à droite. Une mise en correspondance doit être effectuée pour ce bit, ainsi que pour les 16 bits les plus à gauche.

Access-list 1 permit 172.16.0.0 0.0.255.254

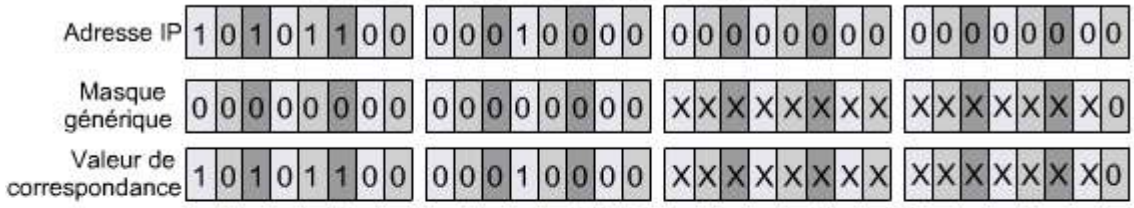


Paquet entrant 172.16.4.1

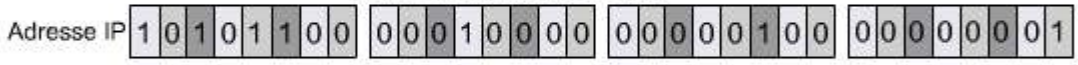


Le premier paquet portant l'adresse 172.16.4.1 accède à l'interface.

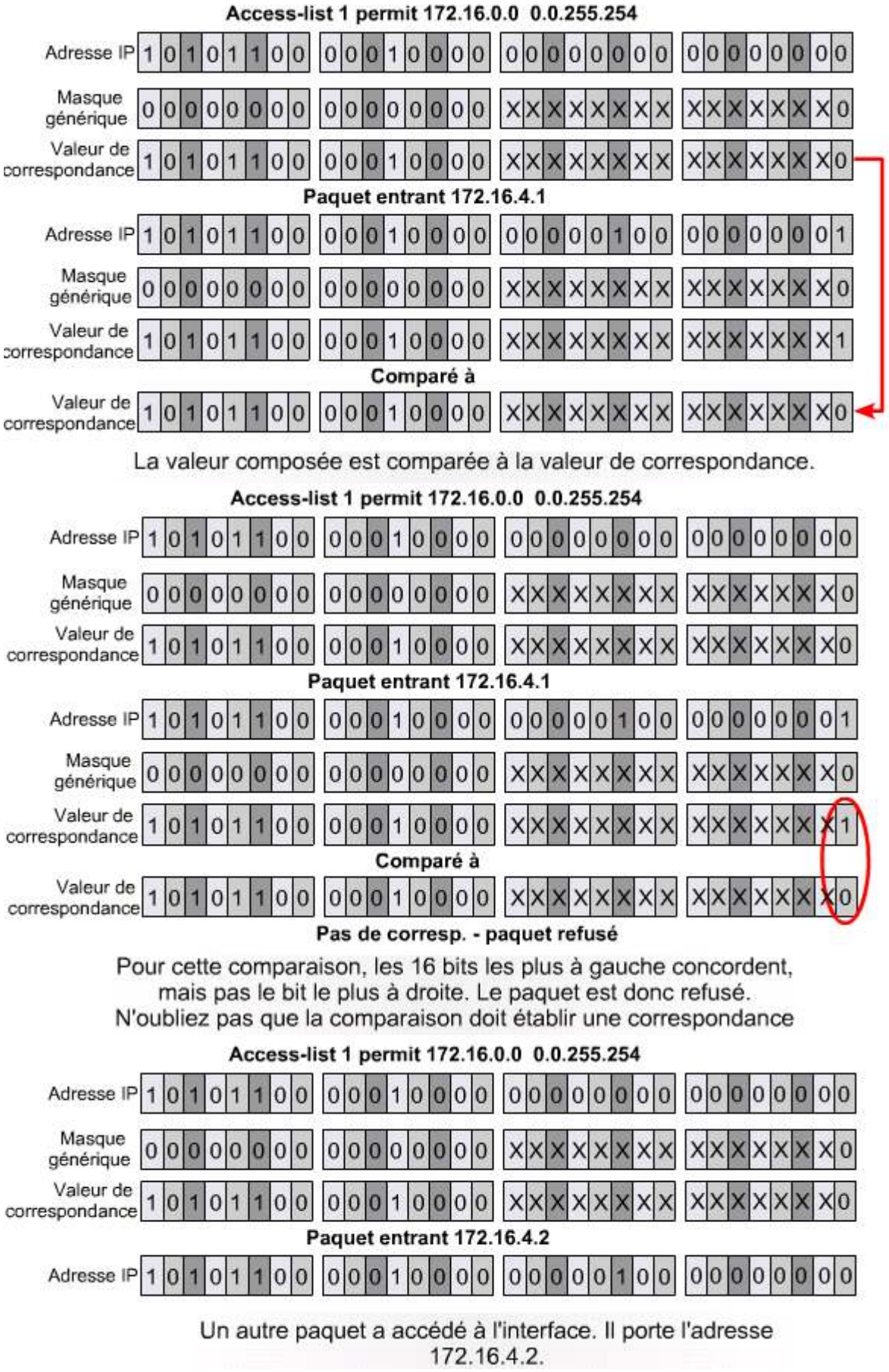
Access-list 1 permit 172.16.0.0 0.0.255.254

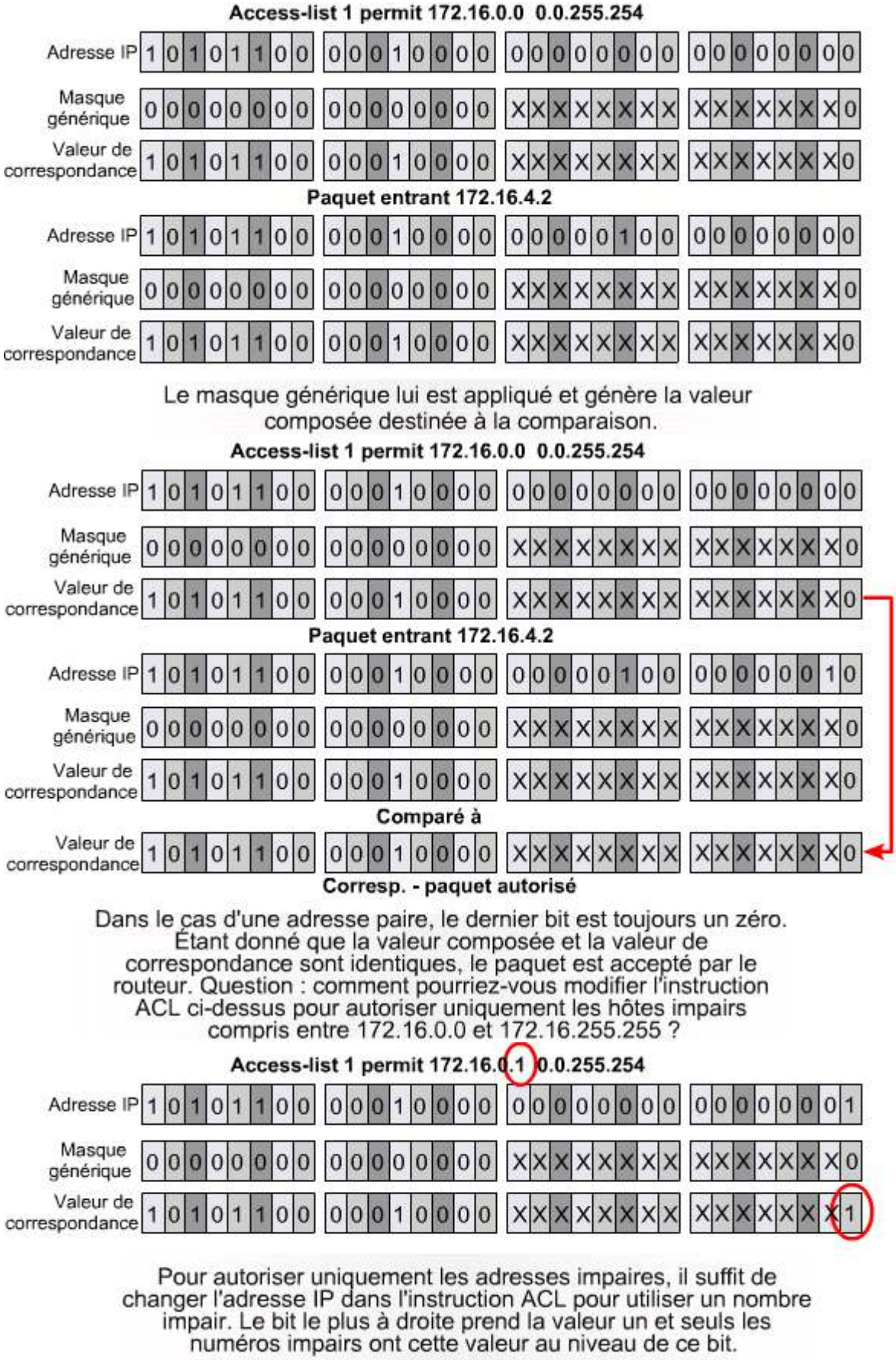


Paquet entrant 172.16.4.1



Le masque générique ACL est appliqué et génère la valeur composée destinée à la comparaison.


Access-list 1 permit 172.16.0.0 0.0.255.254
Adresse IP 10101100 00010000 00000000 00000000
Masque générique 00000000 00000000 XXXXXXXX XXXXXXX0
Valeur de correspondance 10101100 00010000 XXXXXXXX XXXXXXX0
Paquet entrant 172.16.4.1
Adresse IP 10101100 00010000 00000100 00000001
Masque générique 00000000 00000000 XXXXXXXX XXXXXXX0
Valeur de correspondance 10101100 00010000 XXXXXXXX XXXXXXX1
Comparé à
Valeur de correspondance 10101100 00010000 XXXXXXXX XXXXXXX0
La valeur composée est comparée à la valeur de correspondance.
Access-list 1 permit 172.16.0.0 0.0.255.254
Adresse IP 10101100 00010000 00000000 00000000
Masque générique 00000000 00000000 XXXXXXXX XXXXXXX0
Valeur de correspondance 10101100 00010000 XXXXXXXX XXXXXXX0
Paquet entrant 172.16.4.1
Adresse IP 10101100 00010000 00000100 00000001
Masque générique 00000000 00000000 XXXXXXXX XXXXXXX0
Valeur de correspondance 10101100 00010000 XXXXXXXX XXXXXXX1
Comparé à
Valeur de correspondance 10101100 00010000 XXXXXXXX XXXXXXX0
Pas de corresp. - paquet refusé
Pour cette comparaison, les 16 bits les plus à gauche concordent, mais pas le bit le plus à droite. Le paquet est donc refusé.
N'oubliez pas que la comparaison doit établir une correspondance
Access-list 1 permit 172.16.0.0 0.0.255.254
Adresse IP 10101100 00010000 00000000 00000000
Masque générique 00000000 00000000 XXXXXXXX XXXXXXX0
Valeur de correspondance 10101100 00010000 XXXXXXXX XXXXXXX0
Paquet entrant 172.16.4.2
Adresse IP 10101100 00010000 00000100 00000000
Un autre paquet a accédé à l'interface. Il porte l'adresse 172.16.4.2.



Deux mots-clés spéciaux sont utilisés dans les listes de contrôle d'accès, les options **`any`** et **`host`**. 4 L'option **`any`** remplace 0.0.0.0 dans l'adresse IP et 255.255.255.255 dans le masque générique. Cette option établit une correspondance avec toute adresse avec laquelle elle est comparée. L'option **`host`** remplace le masque 0.0.0.0. Ce masque nécessite une correspondance parfaite entre tous les bits de l'adresse ACL et ceux de l'adresse du paquet. Avec cette option, une seule adresse concorde.

```
Router(config)#access-list 1 permit 0.0.0.0
255.255.255.255
```
Peut être écrit comme suit :

```
Router(config)#access-list 1 permit any

Router(config)#access-list 1 permit 172.30.16.29 0.0.0.0
```
Peut être écrit comme suit :

Ceci est le format des mots-clés optionnels **any** et **host** dans une instruction de liste d'accès (ACL).

Activité de média interactive

Glisser-Positionner : Création de listes de contrôle d'accès

À la fin de cette activité, l'étudiant sera en mesure de créer des ACL.

11.1 Notions de base sur la liste de contrôle d'accès (ACL)

11.1.5 Vérification des listes de contrôle d'accès

De nombreuses commandes **show** permettent de vérifier le contenu et l'emplacement des listes de contrôle d'accès sur le routeur.

```
Router#show ip interface
FastEthernet0/0 is up, line protocol is down
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 2
Serial0/0 is down, line protocol is down
  Internet address is 200.200.2.1/24
  Broadcast address is 255.255.255.255
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is 101
```

Extrait d'une commande show ip interface indiquant les affectations d'interface de liste d'accès

La commande **show ip interface** affiche les informations relatives à l'interface IP et indique si des listes de contrôle d'accès sont configurées. 1 La commande **show access-lists** affiche le contenu de toutes les listes de contrôle d'accès sur le routeur. 2

Informations affichées par la commande show access-lists indiquant les deux listes de contrôle d'accès configurées

Pour afficher une liste spécifique, ajoutez le nom ou le numéro de la liste de contrôle d'accès en tant qu'option de cette commande. La commande **show running-config** permet également d'afficher les listes d'accès d'un routeur, ainsi que les informations d'affectation aux interfaces. 3

```
Router#show running-config
Current configuration : 953 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
memory-size iomem 15
ip subnet-zero
no ip finger
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 2 in
!
interface Serial0/0
 ip address 200.200.2.1 255.255.255.0
 ip access-group 101 in
!
access-list 2 deny   172.16.1.1
access-list 2 permit 172.16.1.0 0.0.0.255
access-list 2 deny   172.16.0.0 0.0.255.255
access-list 2 permit 172.0.0.0 0.255.255.255
access-list 101 permit tcp 192.168.6.0 0.0.0.255 any
eq telnet
access-list 101 permit tcp 192.168.6.0 0.0.0.255 any
eq ftp
!
line con 0
 transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end
```

Informations affichées par la commande show access-lists indiquant les deux listes de contrôle d'accès configurées

Ces commandes show vérifient le contenu et l'emplacement des listes. Il est également conseillé de tester les listes d'accès avec des exemples de trafic afin de vérifier leur logique.

Activité de TP

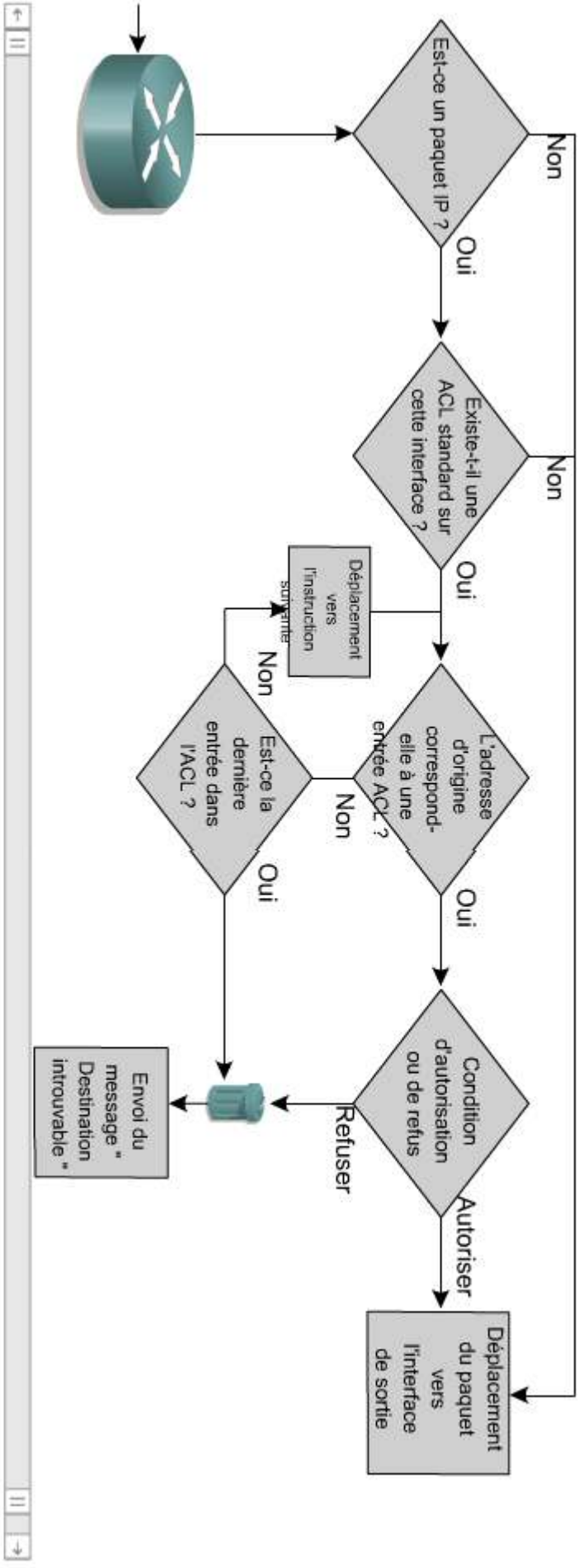
Activité en ligne : Vérification des listes de contrôle d'accès

Au cours de ce TP, les étudiants vont vérifier les listes de contrôle d'accès configurées sur le routeur.

11.2 Listes de contrôle d'accès (ACL)

11.2.1 Listes de contrôle d'accès standard

Les listes d'accès standard vérifient l'adresse d'origine des paquets IP qui sont routés. 1 Selon le résultat de la comparaison, l'acheminement est autorisé ou refusé pour un ensemble de protocoles complet en fonction des adresses réseau, de sous-réseau et d'hôte. À titre d'exemple, l'adresse d'origine et le protocole des paquets qui entrent par l'interface Fa0/0 sont vérifiés. Si l'accès leur est accordé, les paquets sont acheminés à travers le routeur vers une interface de sortie. Dans le cas contraire, ils sont abandonnés au niveau de l'interface d'entrée.

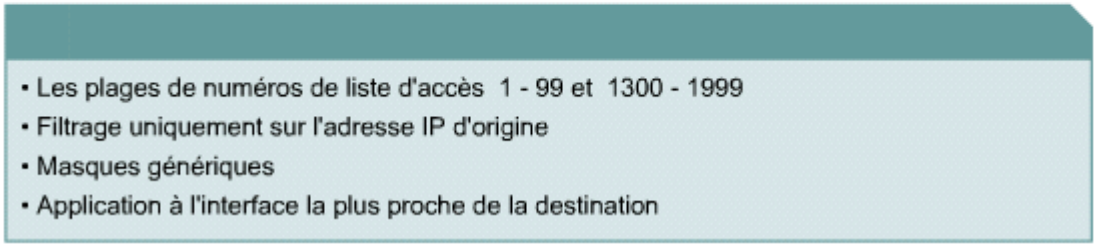


Fenêtre contextuelle

Une ACL de routage standard ne traite que les paquets IP. Elle examine ensuite séquentiellement la liste des instructions. Si aucune correspondance n'est trouvée, le paquet est abandonné. Si l'adresse d'origine du paquet est trouvée, la condition d'autorisation ou de refus est appliquée. S'il ne s'agit pas d'un paquet IP, s'il n'existe pas d'ACL ou si le paquet est autorisé par l'ACL, il est envoyé vers l'algorithme de routage ; sinon, il est éliminé.

La version standard de la commande de configuration globale **access-list** est utilisée pour définir une ACL standard avec un numéro compris entre 1 et 99 À partir de la version Cisco IOS Software Release 12.0.1, les ACL standards ont débuté à utiliser la plage additionnelle (1300 à 1999) afin de procurer un maximum de 798 nouvelles ACL standards. Ces numéros additionnels sont habituellement appelés ACL IP expansées.

```
access-list 2 deny   172.16.1.1
access-list 2 permit 172.16.1.0  0.0.0.255
access-list 2 deny   172.16.0.0  0.0.255.255
access-list 2 permit 172.0.0.0   0.255.255.255
```



Notez que la première instruction ACL ne contient aucun masque générique. Dans le cas où aucune liste n'apparaît, le masque par défaut (0.0.0.0) est utilisé. Cela signifie que la totalité de l'adresse doit correspondre, ou que cette ligne de l'ACL ne s'applique pas et que le routeur doit rechercher une correspondance dans la ligne suivante de la liste d'accès.

La syntaxe complète de la commande ACL standard est la suivante:

```
Router(config)#access-list access-list-number {deny | permit | remark} source
[source-wildcard] [log]
```

Les commentaires **remark** permettent de comprendre plus facilement les listes d'accès. Chaque commentaire est limité à 100 caractères. Par exemple, il n'est pas évident de connaître le but de la saisie :

```
Router(config)#access-list 1 permit 171.69.2.88
```

Il est beaucoup plus facile de lire le commentaire qui suit pour comprendre son effet :

```
Router(config)#Liste d'accès 1 remark Permet seulement au poste de travail de Jones
de passer access-list 1 permit 171.69.2.88
```

Utilisez la forme **no** de cette commande pour supprimer une liste de contrôle d'accès standard. En voici la syntaxe:

```
Router(config)#no access-list numéro-liste-d'accès
```

La commande **ip access-group** applique une ACL standard existante à une interface:

```
Router(config)#ip access-group {access-list-number | access-list-name} {in | out}
```

Le tableau décrit les paramètres utilisés dans cette syntaxe.

Paramètre	Description
access-list-number	Numéro d'une liste d'accès (ACL). Il s'agit d'un nombre de 1 à 99 (pour une liste d'accès standard) et de 1300 à 1999 (pour la plage supplémentaire octroyée pour les listes d'accès standards).
deny	Refuse l'accès si les conditions sont respectées.
permit	Autorise l'accès si les conditions sont respectées.
remark	Ajouter une note remark à propos des instructions dans une liste d'accès facilite la lecture et la compréhension.
source	Numéro du réseau ou de l'hôte d'où provient le paquet. Il existe deux façons d'indiquer la source : ·Utiliser une quantité de 32 bits en notation décimale à quatre parties. ·Utiliser le mot-clé any comme abréviation d'une source et la chaîne-générique-source 0.0.0.0 255.255.255.255. *source-wildcard* of 0.0.0.0 255.255.255.55.
source-wildcard	(Facultatif) Bits génériques à appliquer à la source. Il existe deux façons d'indiquer la chaîne-générique-source : ·Utiliser une quantité de 32 bits en notation décimale à quatre parties. Placer des uns dans les positions de bit à ignorer. ·Utiliser le mot-clé any comme abréviation d'une source et chaîne-générique-source de 0.0.0.0 255.255.255.255.
log	(Facultatif) Provoque un message de journalisation informatif au sujet du paquet correspondant à l'entrée à envoyer au port console. (Le niveau des messages consignés au port console est déterminé par la commande logging console.) Le message indique le numéro de liste de contrôle d'accès, si le paquet a été autorisé ou refusé, l'adresse d'origine et le nombre de paquets. Le message est généré pour le premier paquet pour lequel il y a correspondance, puis par intervalles de cinq minutes, et comprend le nombre de paquets autorisés ou refusés dans l'intervalle de cinq minutes précédent.

Ce tableau indique la syntaxe et les options dans la commande ACL standard.

Activité de TP

Exercice : Configuration de listes d'accès standard

Au cours de ce TP, l'étudiant va configurer et appliquer une liste de contrôle d'accès standard en vue d'autoriser ou de refuser un type de trafic particulier.

Activité de TP

Exercice : Listes de contrôle d'accès standard

Au cours de ce TP, l'étudiant va planifier, configurer et appliquer une liste de contrôle d'accès standard en vue

d'autoriser ou de refuser un type de trafic particulier. L'étudiant testera ensuite la liste de contrôle d'accès pour déterminer si les résultats escomptés ont été atteints.

Activité de TP

Activité en ligne : Configuration d'une liste de contrôle d'accès standard

Au cours de ce TP, les étudiants vont planifier, configurer et appliquer une liste de contrôle d'accès standard pour autoriser ou refuser un certain type de trafic et tester la liste pour déterminer si les résultats escomptés ont été atteints.

Activité de TP

Activité en ligne : ACL standard

Au cours de ce TP, les étudiants vont configurer une liste d'accès standard pour le routeur local "Rome".

Activité de TP

Activité en ligne : ACL standard

Au cours de ce TP, les étudiants vont configurer une liste d'accès standard pour le routeur local "Athènes".

Activité de TP

Activité en ligne : ACL standard

Au cours de ce TP, les étudiants vont configurer une liste d'accès standard pour le routeur local "Bucharest".

Activité de TP

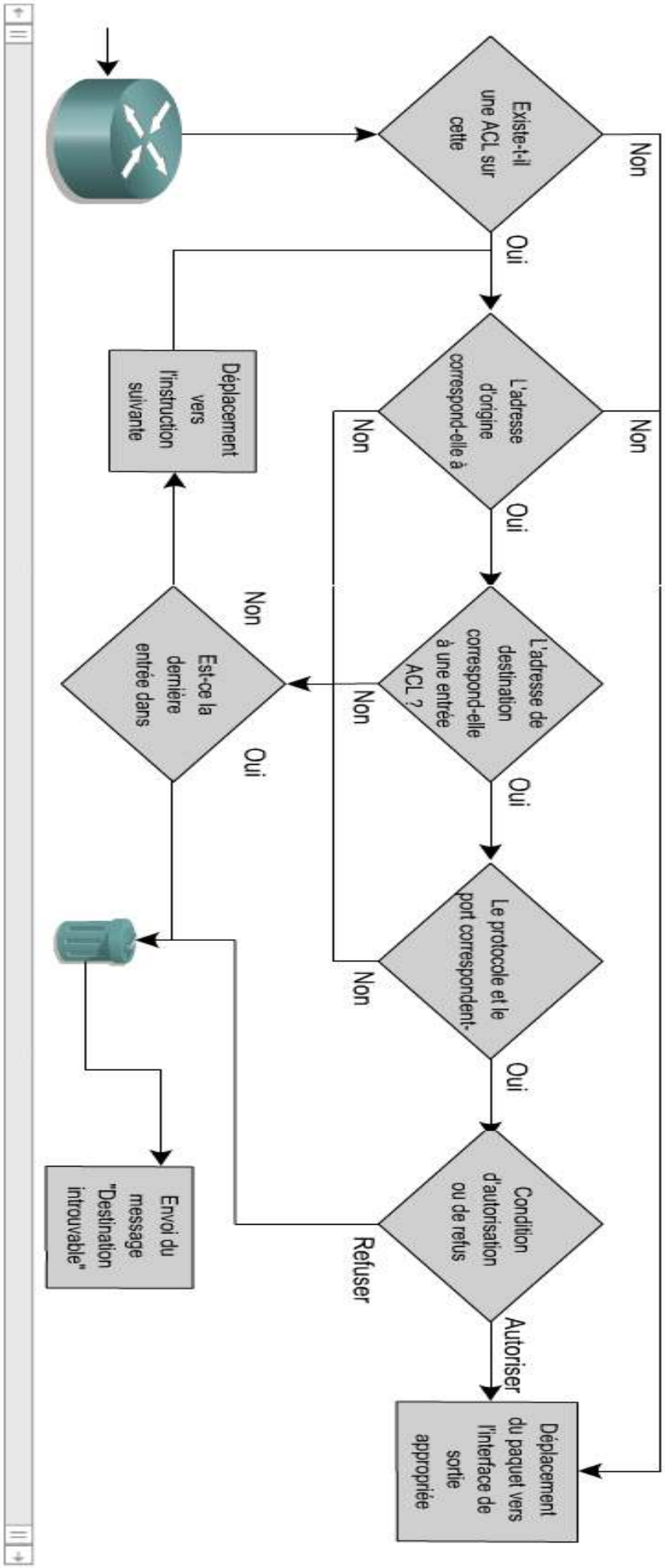
Activité en ligne : ACL standard

Au cours de ce TP, les étudiants vont configurer une liste d'accès standard pour le routeur local "Sofia".

11.2 Listes de contrôle d'accès (ACL)

11.2.2 Listes de contrôle d'accès étendues

Les listes d'accès étendues sont utilisées plus souvent que les listes d'accès standard car elles fournissent une plus grande gamme de contrôle. 1 Les listes d'accès étendues vérifient les adresses d'origine et de destination du paquet, mais peuvent aussi vérifier les protocoles et les numéros de port. Cela donne une plus grande souplesse pour décrire ce que vérifie la liste de contrôle d'accès. L'accès d'un paquet peut être autorisé ou refusé selon son emplacement d'origine et sa destination, mais aussi selon son type de protocole et les adresses de ses ports. Une liste de contrôle d'accès étendue peut autoriser le trafic de messagerie issu de l'interface Fa0/0 vers des destinations S0/0 données tout en refusant des transferts de fichiers et des navigations sur le Web. Lorsque des paquets sont éliminés, certains protocoles envoient un paquet d'écho à l'émetteur, pour lui indiquer que la destination était inaccessible.


Existe-t-il une ACL sur cette
Non
Oui
L'adresse d'origine correspond-elle à
Non
Non
Oui
Déplacement vers l'instruction suivante
L'adresse de destination correspond-elle à une entrée ACL ?
Non
Oui
Est-ce la dernière entrée dans
Non
Oui
Le protocole et le port correspondent-
Non
Oui
Condition d'autorisation ou de refus
Refuser
Autoriser
Envoi du message "Destination introuvable"
Déplacement du paquet vers l'interface de sortie appropriée

Pour une même liste de contrôle d'accès, plusieurs instructions peuvent être configurées. 2 Chacune de ces instructions doit contenir le même numéro de liste d'accès pour que toutes les instructions soient associées à la même liste de contrôle d'accès. Vous pouvez définir autant d'instructions que vous le souhaitez, la seule limite étant la mémoire disponible sur le routeur. Il va sans dire que plus il y a d'instructions, plus la liste de contrôle d'accès est difficile à comprendre et à gérer.

```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

- Les plages de numéros de liste d'accès 100-199 et 2000 - 2699
- Adresse IP de destination source
- Numéro de protocole de couche 4
- Application au port le plus proche de l'hôte source

La syntaxe d'une instruction de liste d'accès étendue peut être très longue et fait souvent l'objet de retours à la ligne automatiques dans la fenêtre du terminal. Les masques génériques permettent également d'utiliser les mots-clés **`host`** ou **`any`** dans la commande. 3

```
access-list access-list-number [dynamic dynamic-name [timeout
minutes]] {deny | permit | remark} protocol source source-
wildcard destination destination-wildcard [precedence
precedence] [tos tos] [log | log-input] [time-range time-
range-name] icmp-type icmp-code icmp-message igmp-type
[operator operand] [port port number or name] [established]
[fragments]
```

Paramètre	Description
access-list-number	Identifie la liste avec un nombre de 100 à 199 (pour une liste d'accès étendue) et de 2000 à 2699 (pour la plage supplémentaire octroyée pour les listes d'accès étendues).
dynamic *dynamic-name*	(Facultatif) identifie cette liste d'accès comme une liste d'accès dynamique.
timeout *minutes*	(Facultatif) spécifie la durée absolue, en minutes, qu'une déclaration provisoire de la liste d'accès peut rester dans une liste d'accès dynamique. La valeur par défaut spécifie une durée infinie et permet à une déclaration d'y rester de manière permanente.
deny	deny interdit l'accès si les conditions correspondent.
permit	permet l'accès si les conditions correspondent.
remark	Indique si l'instruction permet ou empêche l'adresse spécifiée. Pourrait aussi être utilisé pour entrer une note.
protocol	spécifie le nom ou le numéro d'un protocole Internet. Il ne peut qu'être l'un des mots clé suivants : eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, pim, tcp, ou udp, ou un entier compris entre 0 et 255, spécifiant le numéro de protocol Internet. Pour l'équivalence avec un quelconque protocole Internet (incluant ICMP, TCP et UDP) utiliser le mot-clé ip.
source	source spécifie le numéro du réseau ou d'host d'où le paquet a été envoyé. Il y a trois alternatives pour spécifier la source : • utiliser 32 bits au format "décimal point". • Utiliser le mot-clé any comme abréviation de la *source* et 0.0.0.0 255.255.255.255 pour *source-wildcard*. • Utiliser **host** comme abréviation de la *source* et 0.0.0.0 pour *source-wildcard*.

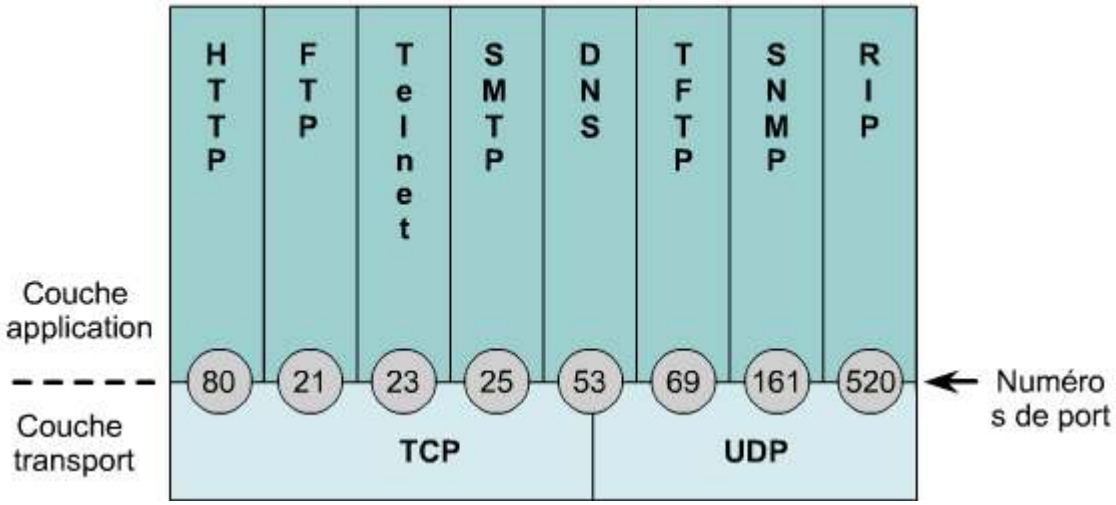
source-wildcard	spécifie les 32 bits de test de correspondance appliqués à source. Chaque bit de test de correspondance à 0 indique la position d'un bit d'équivalence pour la source. Chaque bit de test de correspondance à 1 indique qu'un bit à 0 ou un bit à 1 en position correspondante de l'adresse IP du paquet sera considéré équivalent dans cette déclaration de liste d'accès. Il y a trois alternatives pour spécifier le source-wildcard : • utiliser 32 bits au format "décimal point". Forcer à "1" les bits de test de correspondance pour lesquels vous voulez ignorer l'équivalence. • Utiliser le mot-clé any comme abréviation de la *source* et 0.0.0.0 255.255.255.255 pour *source-wildcard*. • Utiliser **host** comme abréviation de la *source* et 0.0.0.0 pour *source-wildcard*. Les bits positionnés à 1 dans le masque générique ne doivent pas être obligatoirement contigus dans le masque générique source. Par exemple, un masque générique source 0.255.0.64 est valable.
destination	spécifie le numéro du réseau ou d'host auquel le paquet est envoyé. Il y a trois alternatives pour spécifier la destination : • utiliser 32 bits au format "décimal point". • Utiliser le mot-clé any comme abréviation de la *source* et 0.0.0.0 255.255.255.255 pour *source-wildcard*. • Utiliser **host** comme abréviation de la *source* et 0.0.0.0 pour *source-wildcard*.

destination-wildcard	Bits du masque générique appliqué à la destinationIl y a trois alternatives pour spécifier le destination-wildcard : • utiliser 32 bits au format "décimal point". Forcer à "1" les bits de test de correspondance pour lesquels vous voulez ignorer l'équivalence. • Utiliser le mot-clé any comme abréviation de la *source* et 0.0.0.0 255.255.255.255 pour *source-wildcard*. • Utiliser **host** comme abréviation de la *source* et 0.0.0.0 pour *source-wildcard*.
precedence *precedence*	(Facultatif) des paquets peuvent être filtrés à l'aide du niveau de préséance (priorité), spécifié par un nombre de 0 à 7, ou par un nom.
tos *tos*	(Facultatif) des paquets peuvent être filtrés à l'aide du niveau de service, spécifié par un nombre de 0 à 15, ou par un nom.
log	(Facultatif) affiche sur la console un message d'enregistrement d'informations du paquet qui répond à une déclaration Le niveau des messages de log envoyés à la console est contrôlé par la commande "**login console**". Le message inclut le numéro de liste d'accès, que le paquet soit permis ou interdit; que le protocole soit TCP, UDP, ICMP ou un nombre; et si c'est approprié, les adresses source et destination et les numéros de port source et destination. Le message se produit dès le premier paquet qui répond aux conditions d'équivalence puis à intervalles de 5 minutes, incluant le nombre de paquets permis ou interdits dans l'intervalle antérieur de 5 minutes. Une session de Log peut rater quelques messages s'il y en a trop à traiter ou s'il y a plus d'un à traiter par seconde. Cela empêche le routeur de s'effondrer en présence de trop de paquets de Log. Donc, une session Log ne doit pas être utilisée comme outil de facturation ou un comme source précise du nombre d'équivalences par liste d'accès

log-input	(Facultatif) inclut l'interface d'entrée et l'adresse source MAC ou VC dans la production des enregistrements. time-range time-range-name
time-range *time-range-name*	(Facultatif) spécifie le nom de la gamme de temps qui s'applique à cette déclaration. Le nom de la gamme de temps et ses restrictions sont spécifiés par la commande <B><FONT FACE="Courier
icmp-type	(Facultatif) des paquets ICMP peuvent être filtrés par le type de message ICMP. Le type est un nombre compris entre 0 et 255.
icmp-code	(Facultatif) les paquets ICMP qui sont filtrés par le type de message ICMP peuvent être aussi filtrés par le code du message ICMP. Le code est un nombre compris entre 0 et 255.
icmp-message	(Facultatifs) les paquets ICMP peuvent être filtrés à l'aide du nom du type de message ICMP ou du nom codé du type de message ICMP.
igmp-type	(Facultatifs) les paquets IGMP peuvent être filtrés à l'aide du type de message ou du nom de message IGMP. Le type de message est un nombre compris entre 0 et 15.
operator	(Facultatif) compare les ports de destination ou de source. Les opérandes possibles incluent **lt** (moins que), **gt** (plus grand que), **eq** (égal), **neq** (non égal) et **range** (gamme inclusive). Si l'opérateur est placé après le **source** et le **source-wildcard**, il doit correspondre au port Si l'opérateur est placé après la **destination** et le **destination-wildcard**, il doit correspondre au port destination. L'opérateur **range** exige deux numéros de port. Tous les autres opérateurs n'exigent qu'un numéro
port	(Facultatif) spécifie le numéro en décimal ou le nom d'un port TCP ou UDP. Un numéro de port est un nombre dompris entre 0 et 65535. Les noms de port TCP et UDP sont listés dans la section "Directives d'Utilisation". Les noms de port TCP ne peuvent être spécifiés que pour un filtrage TCP. Les noms de port UDP ne peuvent être spécifiés que pour un filtrage UDP.
established	(Facultatif) ne s'applique qu"au protocole TCP seulement : indique une connexion établie. L'équivalence se produit si le datagramme TCP possède comme bit de contrôle actif : ACK, FIN, PSH, RST, SYN, or URG. Les cas de non équivalence se produisent avec les datagrammes TCP qui participent à l'établissement de la connexion initiale. fragments
fragments	(Facultatif) la déclaration de la liste d'accès s'applique aux fragments des paquets; en conséquence, le fragment est soit autorisé soit interdit.

Démonstration de la syntaxe d'une liste de contrôle d'accès étendue et explication des paramètres

À la fin de l'instruction de liste d'accès étendue, un champ indiquant le numéro de port de protocole TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol) facultatif ajoute de la précision. 4



Les numéros de port bien connus pour TCP/IP sont indiqués dans la figure 5. Des opérateurs logiques peuvent être spécifiés, par exemple égal (eq), non égal (neq), supérieur à (gt) et inférieur à (lt), et appliqués à des protocoles spécifiques. Les listes d'accès étendues utilisent un numéro compris entre 100 et 199 (également entre 2000 et 2699 dans les versions récentes de l'IOS).

Décimal	Mot-clé	Description	TCP ou UDP
0		Réservé	Réservé
1-4		Non attribué	
5	RJE	Soumission de travaux à distance	TCP, UDP
7	ECHO	Écho	TCP, UDP
9	DISCARD	Élimination	TCP, UDP
11	USERS	Utilisateurs actifs	TCP, UDP
13	DAYTIME	Heure du jour	TCP, UDP
15	NETSTAT	Who is Up ou NETSTAT	TCP, UDP
17	QUOTE	Citation du jour	TCP, UDP
19	CHARGEN	Générateur de caractères	TCP, UDP
20	FTP-DATA	Protocole FTP (données)	TCP, UDP
21	FTP	Protocole FTP	TCP, UDP
23	TELNET	Connexion en mode terminal	TCP, UDP
25	SMTP	Protocole SMTP(Simple Mail Transfer Protocol)	TCP, UDP
37	TIME	Heure du jour	TCP, UDP
39	RLP	Protocole RLP (Resource Location Protocol)	TCP, UDP
42	NAMESERVER	Serveur de noms d'hôte	TCP, UDP
43	NICNAME	Who Is	TCP, UDP
53	DOMAIN	Serveur de noms de domaine	TCP, UDP
67	BOOTPS	Serveur de protocole Bootstrap	TCP, UDP
68	BOOTPC	Client de protocole Bootstrap	TCP, UDP
69	TFTP	Protocole TFTP (Trivial File Transfer Protocol)	TCP, UDP
75		Tout service de sortie privé	TCP, UDP
77		Tout service RJE privé	TCP, UDP
79	FINGER	Finger	TCP, UDP
80	HTTP	Protocole HTTP	TCP
95	SUPDUP	Protocole SUPDUP	TCP
101	HOSTNAME	Serveur de noms d'hôte NIC	TCP
102	ISO-TSAP	ISO-TSAP	TCP
110	POP3	Protocole POP (Post Office Protocol)	TCP
113	AUTH	Service d'authentification	TCP
117	UUCP-PATH	Service de chemin UUCP	TCP
123	NTP	Protocole NTP (Network Time Protocol)	TCP, UDP
133-159		Non attribué	Non attribué
160-223		Réservé	Réservé
224-241		Non attribué	Non attribué
242-255		Non attribué	Non attribué

Une liste par interface, par direction, par protocole

La commande **`ip access-group`** lie une liste de contrôle d'accès étendue existante à une interface. N'oubliez pas qu'une seule liste de contrôle d'accès est permise par interface, par direction et par protocole. La syntaxe de cette commande est la suivante:

```
Router(config-if)#ip access-group numéro-liste-d'accès {in | out}
```

Activité de TP

Exercice : Configuration de listes d'accès étendues

L'objectif de ce TP est de configurer et d'appliquer une liste de contrôle d'accès étendue en vue d'autoriser ou de refuser un type de trafic particulier.

Activité de TP

Exercice : Listes d'accès étendues simples

L'objectif de ce TP est de configurer et d'appliquer des listes de contrôle d'accès étendues pour filtrer le trafic réseau/réseau, hôte/réseau et réseau/hôte.

Activité de TP

Activité en ligne : Configuration d'une liste de contrôle d'accès étendue

Au cours de ce TP, l'étudiant va planifier, configurer et appliquer une liste de contrôle d'accès étendue pour autoriser ou refuser un certain type de trafic et tester la liste pour déterminer si les résultats escomptés ont été atteints.

Activité de TP

Activité en ligne : ACL étendue

Au cours de ce TP, les étudiants vont configurer une liste d'accès étendue pour le routeur local "Mexico_City".

Activité de TP

Activité en ligne : ACL étendue

Au cours de ce TP, les étudiants vont configurer une liste d'accès étendue pour le routeur local "Jakarta".

Activité de TP

Activité en ligne : ACL étendue

Au cours de ce TP, les étudiants vont configurer une liste d'accès étendue pour le routeur local "Kuwait".

Activité de TP

Activité en ligne : ACL étendue

Au cours de ce TP, les étudiants vont configurer une liste d'accès étendue pour le routeur local "Abuja".

11.2 Listes de contrôle d'accès (ACL)

11.2.3 Listes de contrôle d'accès nommées

Les listes de contrôle d'accès nommées IP ont été introduites dans la plate-forme logicielle Cisco IOS version 11.2, afin d'attribuer des noms aux listes d'accès standard et étendues à la place des numéros. 1 Les avantages procurés par une liste d'accès nommée sont les suivants:

- Identifier de manière intuitive une liste d'accès à l'aide d'un nom alphanumérique.
- L'IOS ne limite pas le nombre d'ACL nommées qui peuvent être configurées.
- Les ACL nommées permettent de modifier des listes de contrôle d'accès sans avoir à les supprimer, puis à les reconfigurer. Il est important de noter qu'une liste d'accès nommée permet de supprimer des instructions, et d'insérer des instructions uniquement à la fin de la liste. Même avec des listes d'accès nommées, il est préférable d'utiliser un éditeur de texte pour les créer. 2

```
router#configure terminal
Enter configuration commands, one per line.
router(config)#ip access-list extended test
router(config-ext-nacl)#permit ip host 2.2.2.2 host
   3.3.3.3
router(config-ext-nacl)#permit tcp host 1.1.1.1 host
   5.5.5.5 eq www
router(config-ext-nacl)#permit icmp any any
router(config-ext-nacl)#permit udp host 6.6.6.6 10.10.10.0
   0.0.0.255 eq domain
router(config-ext-nacl)#^Z
1d00h: %SYS-5-CONFIG_I: Configured from console by
  consoles-1

router#show access-list
Extended IP access list test
      permit ip host 2.2.2.2 host 3.3.3.3
      permit tcp host 1.1.1.1 host 5.5.5.5 eq www
      permit icmp any any
      permit udp host 6.6.6.6 10.10.10.0 0.0.0.255 eq
      domain

router#configure terminal
Enter configuration commands, one per line. End with
   CNTL/Z.
router(config)#ip access-list extended test
!--- ACL entry deleted.
router(config-ext-nacl)#no permit icmp any any
!--- ACL entry added.
router(config-ext-nacl)#permit gre host 4.4.4.4 host
   8.8.8.8
router(config-ext-nacl)#^Z
1d00h: %SYS-5-CONFIG_I: Configured from console by
   consoles-1

router#show access-list
Extended IP access list test
       permit ip host 2.2.2.2 host 3.3.3.3
       permit tcp host 1.1.1.1 host 5.5.5.5 eq www
       permit udp host 6.6.6.6 10.10.10.0 0.0.0.255 eq
       domain
       permit gre host 4.4.4.4 host 8.8.8.8
```

=

Tout élément supprimé est retiré de la liste de contrôle d'accès et tout élément ajouté est inséré à la fin de la liste.

Prenez en considération les éléments suivants avant de mettre en œuvre des listes de contrôle d'accès nommées.

Les listes de contrôle d'accès nommées ne sont pas compatibles avec les versions de la plate-forme logicielle Cisco IOS antérieures à la version 11.2.

Un même nom ne peut pas être utilisé pour plusieurs listes de contrôle d'accès. Par exemple, il n'est pas possible de spécifier à la fois une ACL standard et une ACL étendue nommée George.

Il est important de connaître les listes d'accès nommées en raison des avantages présentés ci-avant. Le fonctionnement des listes d'accès avancées, telles que les listes d'accès nommées, est présenté dans le cursus CCNP.

Une liste de contrôle d'accès nommée est créée avec la commande **ip access-list**. 3

```
ip access-list {extended|standard} name
```

Syntaxe de commande pour les ACL nommées IP

L'utilisateur passe en mode de configuration d'ACL. En mode de configuration de liste de contrôle d'accès, précisez une ou plusieurs conditions d'autorisation ou de refus. 4

```
router(config-ext-nacl)#permit|deny protocol source
source-wildcard [operator [port]] destination
destination-wildcard [operator [port]] [established]
[precedence precedence] [tos tos] [log] [time-range time-
range-name]
```

Syntaxe d'une instruction d'autorisation et de refus de la commande access-list nommée

Cela détermine si le paquet est acheminé ou abandonné lorsque l'instruction ACL est satisfaite.

La configuration présentée crée une liste de contrôle d'accès standard nommée Internetfilter et une liste de contrôle d'accès étendue nommée marketing_group. La figure 5 illustre également l'application des listes d'accès nommées à une interface.

```
interface ethernet0/5
ip address 192.168.5.1 255.255.255.0
ip access-group Internetfilter out
ip access-group marketing_group in
...
ip access-list standard Internetfilter
permit 10.1.1.1
deny any
ip access-list extended marketing_group
permit tcp any 172.30.0.0. 0.255.255.255 eq telnet
deny udp any any
deny udp any 171.30.0.0. 0.255.255.255 lt 1024
deny ip any log
```

La configuration présentée crée une liste de contrôle d'accès standard nommée Internetfilter et une liste de contrôle d'accès étendue nommée marketing_group. Les listes sont appliquées à l'interface Ethernet 0/5.

Activité de TP

Exercice : Configuration d'une liste de contrôle d'accès nommée

Au cours de ce TP, l'étudiant va créer une liste de contrôle d'accès nommée en vue d'autoriser ou de refuser un type de trafic particulier.

Activité de TP

Exercice : Listes de contrôle d'accès étendues pour les zones DMZ (zones démilitarisées) simples

Au cours de ce TP, l'étudiant va utiliser des listes de contrôle d'accès étendues pour créer une zone DMZ (ou zone démilitarisée) simple.

Activité de TP

Exercice : Fonctions des listes de contrôle d'accès multiples (TP avancé)

Au cours de ce TP, l'étudiant va configurer et appliquer une liste de contrôle d'accès étendue pour contrôler le trafic Internet à l'aide d'un ou de plusieurs routeurs.

Activité de TP

Activité en ligne : Liste de contrôle d'accès nommée

Au cours de ce TP, les étudiants vont configurer une liste de contrôle d'accès nommée pour le routeur local "Ouagadougou".

Activité de TP

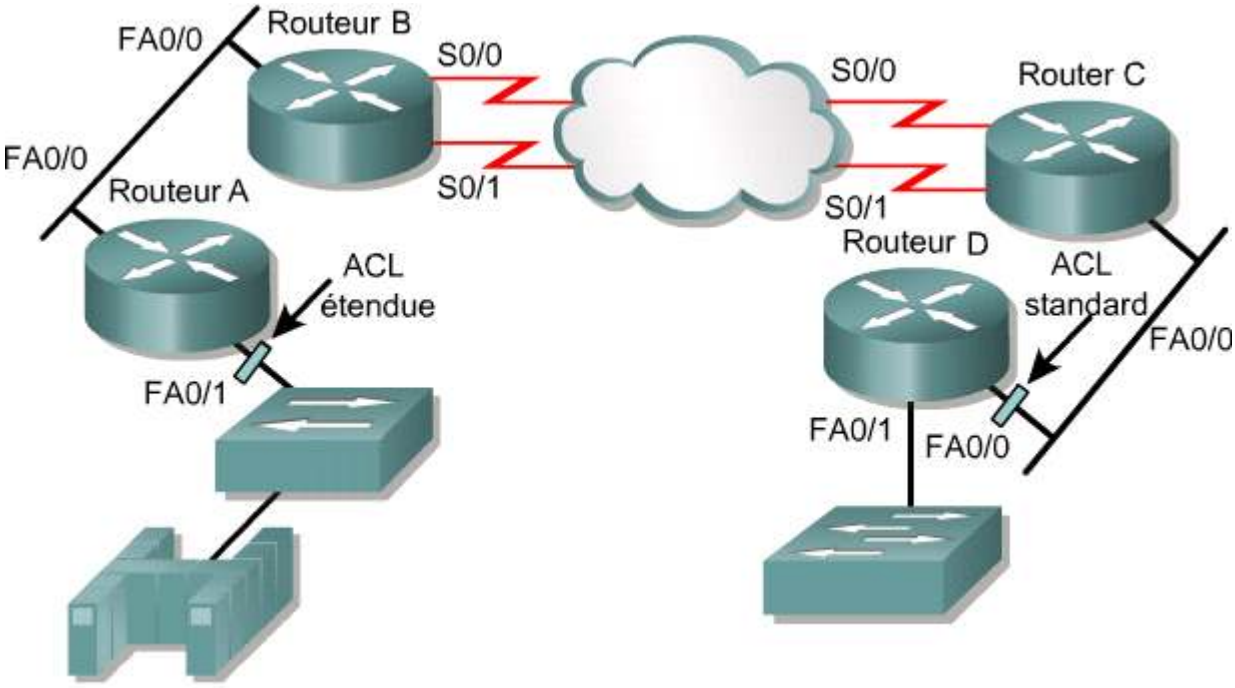
Activité en ligne : Configuration d'une liste de contrôle d'accès nommée
Au cours de ce TP, les étudiants vont créer une liste de contrôle d'accès nommée pour autoriser ou refuser un certain

type de trafic et tester la liste pour déterminer si les résultats escomptés ont été atteints.

11.2 Listes de contrôle d'accès (ACL)

11.2.4 Emplacement des listes de contrôle d'accès

Les listes de contrôle d'accès sont utilisées pour contrôler le trafic en filtrant les paquets et en éliminant le trafic indésirable sur un réseau. Un autre élément à considérer lors de la mise en œuvre des listes de contrôle d'accès est l'emplacement de ces listes. Si les listes de contrôle d'accès sont correctement placées, non seulement le trafic peut être filtré, mais tout le réseau devient plus performant. Si le trafic est filtré, la liste de contrôle d'accès doit être placée à l'endroit où elle aura le plus grand impact sur les performances.



À la figure 1, l'administrateur désire refuser le trafic Telnet ou FTP à partir d'un segment LAN Ethernet du routeur A vers l'interface Fa0/1 LAN Ethernet commutée du routeur D, alors qu'en même temps tout autre trafic doit être autorisé. Diverses approches peuvent permettre d'atteindre cet objectif. L'approche recommandée est l'utilisation d'une liste de contrôle d'accès étendue indiquant les adresses d'origine et de destination. Placez cette liste de contrôle d'accès étendue dans le routeur A. Ainsi, les paquets ne traverseront pas l'Ethernet du routeur A, ni les interfaces série des routeurs B et C. En conséquence, ils ne pénétreront pas dans le routeur D. Le trafic comportant des adresses d'origine et de destination différentes sera encore autorisé.

La règle générale est de placer les listes de contrôle d'accès étendues le plus près possible de la source du trafic refusé. Étant donné que les listes de contrôle d'accès standard ne précisent pas les adresses de destination, vous devez les placer le plus près possible de la destination. Ainsi, vous devriez placer une liste de contrôle d'accès standard sur le port Fa0/0 du routeur D pour interdire le trafic provenant du routeur A.

Un administrateur ne peut placer une liste d'accès que sur une unité qu'il contrôle. Par conséquent, l'emplacement des listes d'accès doit être déterminé dans le contexte dans lequel s'étend le contrôle de l'administrateur réseau.

Activité de média interactive

Pointer-cliquer : Placement de listes de contrôle d'accès

À la fin de cette activité, l'étudiant sera en mesure de placer des listes de contrôle d'accès.

11.2 Listes de contrôle d'accès (ACL)

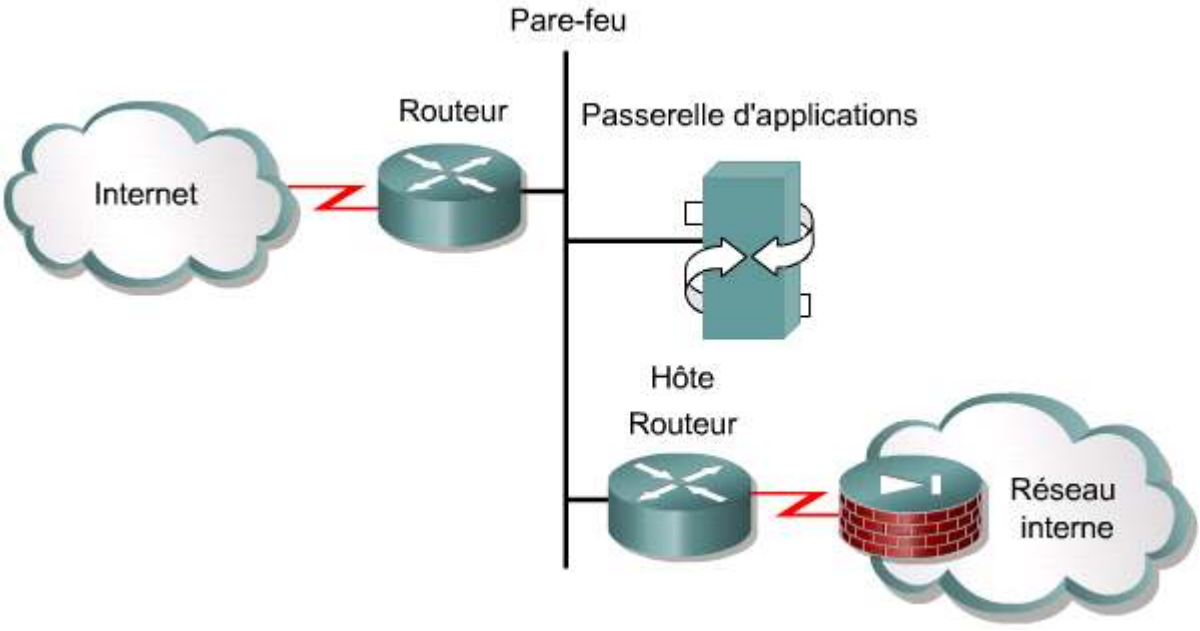
11.2.5 Pare-feu

Un pare-feu est une structure située entre l'utilisateur et le monde extérieur afin de protéger le réseau interne des intrus. Dans la plupart des cas, les intrus proviennent du réseau global Internet et des milliers de réseaux distants qu'il interconnecte. En règle générale, un pare-feu réseau est constitué de plusieurs machines différentes qui travaillent ensemble pour empêcher l'accès indésirable et non autorisé.

Dans l'architecture présentée, le routeur connecté au réseau Internet, appelé routeur externe, oblige tout le trafic entrant à passer par la passerelle d'application. Le routeur connecté au réseau interne, appelé routeur hôte, accepte uniquement les paquets de la passerelle d'application. En fait, la passerelle gère la livraison des services réseau vers le réseau interne et à partir de celui-ci. Par exemple, seuls certains utilisateurs peuvent être autorisés à se connecter à Internet ou seules certaines applications peuvent être autorisées à établir des connexions entre des hôtes internes et externes. Si la seule application autorisée est la messagerie électronique, le routeur doit autoriser uniquement le passage des paquets de courrier. Cela protège la passerelle d'application et évite de l'inonder avec des paquets qu'elle abandonnerait autrement.

Les listes de contrôle d'accès doivent être utilisées dans les routeurs pare-feu, lesquels sont souvent placés entre le réseau interne et un réseau externe, tel qu'Internet. Cela permet ainsi de contrôler le trafic entrant ou sortant d'un endroit spécifique du réseau interne. Vous pouvez également utiliser les listes de contrôle d'accès sur un routeur situé entre deux sections du réseau pour contrôler le trafic entrant ou sortant d'une section particulière du réseau interne.

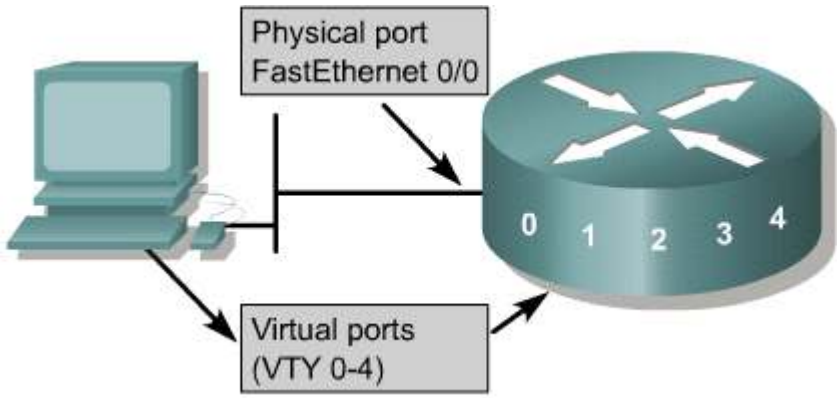
Vous devez configurer des listes de contrôle d'accès sur les routeurs périphériques situés aux frontières du réseau pour tirer parti des avantages des listes de contrôle d'accès en matière de sécurité. Cela permet de fournir une protection de base contre le réseau externe ou de mettre à l'abri une zone plus privée du réseau d'une zone moins contrôlée. Sur ces routeurs périphériques, des listes de contrôle d'accès peuvent être créées pour chaque protocole réseau configuré sur les interfaces des routeurs.



11.2 Listes de contrôle d'accès (ACL)

11.2.6 Restriction de l'accès au terminal virtuel

Les listes d'accès standard et étendues s'appliquent aux paquets traversant un routeur. 1Elles ne sont pas destinées à bloquer les paquets qui sont créés sur ce routeur. Par défaut, une liste d'accès étendue pour le trafic Telnet sortant n'empêche pas le routeur de lancer des sessions Telnet.



Tout comme il existe des interfaces ou des ports physiques, tels que Fa0/0 et S0/0 sur le routeur, il existe également des ports virtuels. Ces ports virtuels sont appelés lignes vty. Il existe cinq lignes vty, numérotées de 0 à 4, comme l'indique la figure 1 . Pour des raisons de sécurité, l'accès au terminal virtuel du routeur peut être autorisé ou refusé aux utilisateurs, mais l'accès à des destinations à partir de ce routeur peut leur être refusé.

L'objectif de l'accès limité au terminal virtuel est d'augmenter la sécurité du réseau. L'accès au terminal virtuel est également possible avec le protocole Telnet qui crée une connexion non physique vers le routeur. Ainsi, il n'existe qu'un seul type de liste de contrôle d'accès au terminal virtuel. Des restrictions identiques doivent être définies sur toutes les lignes vty, car il n'est pas possible de contrôler la ligne à laquelle l'utilisateur va se connecter.

Le processus de création de la liste de contrôle d'accès au terminal virtuel est identique à celui décrit pour une interface. Toutefois, l'application de la liste de contrôle d'accès à une ligne de terminal nécessite la commande **`access-class`** à la place de la commande **`access-group`**. 2

Cisco - Hyperterminal

```
Creating the standard list:

Rtl(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Rtl(config)#access-list 2 permit 172.16.2.0 0.0.0.255
Rtl(config)#access-list 2 deny any

Applying the access list:

Rtl(config)#line vty 0 4
Rtl(config-line)#login
Rtl(config-line)#password secret
Rtl(config-line)#access-class 2 in
```

Vous devez prendre en compte les éléments suivants lors de la configuration de listes d'accès sur des lignes vty :

- Lors du contrôle de l'accès à une interface, un nom ou un numéro peut être utilisé.
- Seules les listes d'accès numérotées peuvent être appliquées à des lignes virtuelles.

- Définissez des restrictions identiques sur toutes les lignes de terminal virtuel, car un utilisateur peut tenter de se connecter à n'importe quelle ligne.

Activité de TP

Exercice : Restrictions applicables aux terminaux virtuels (VTY)

Au cours de ce TP, l'étudiant va utiliser les commandes access-class et line pour contrôler l'accès au routeur via telnet.

Activité de TP

Activité en ligne : Listes de contrôle d'accès

Au cours de ce TP, les étudiants vont mettre en pratique l'utilisation des listes de contrôle d'accès pour filtrer le trafic IP.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Les listes de contrôle d'accès remplissent plusieurs fonctions à l'intérieur d'un routeur, y compris la mise en œuvre de procédures de sécurité et d'accès.
- Les listes de contrôle d'accès sont utilisées pour contrôler et gérer le trafic.
- Dans le cas de certains protocoles, vous pouvez appliquer deux listes de contrôle d'accès à une interface : une liste d'accès qui contrôle le trafic entrant et une autre qui contrôle le trafic sortant.
- Avec ces listes, dès qu'une correspondance est établie avec une instruction ACL, l'accès au routeur peut être autorisé ou refusé au paquet en question.
- Les bits de masque générique utilisent les chiffres 1 et 0 pour préciser la façon de traiter les bits correspondants de l'adresse IP.
- La création et l'application des listes d'accès sont vérifiées par l'utilisation de commandes show IOS variées.
- Les deux principaux types de liste de contrôle d'accès sont les listes de contrôle d'accès standard et les listes de contrôle d'accès étendues.
- Les listes de contrôle d'accès nommées permettent d'utiliser un nom pour identifier la liste au lieu d'un numéro.
- Des listes de contrôle d'accès peuvent être configurées pour tous les protocoles réseau routés.
- Les listes de contrôle d'accès sont placées là où elles permettent un contrôle optimum.
- Les listes de contrôle d'accès sont généralement utilisées dans les routeurs pare-feu.
- Les listes de contrôle d'accès peuvent également limiter l'accès au terminal virtuel du routeur.